Update: 26/04/2021

April 12 - 23, 2021: Hanoi (Vietnam) (online)
CIMPA School on Functional Equations: Theory, Practice and Interaction.

Introduction to transcendental numbers

Michel Waldschmidt

1 Criteria for irrationality and for transcendence

1.1 Irrationality criterion

Most constants arising from analysis involve limits, infinite series or products, integrals. For such numbers, the classical irrationality criteria using expansions in a basis $b \geq 2$ or the continued fraction expansion are of no use. The most efficient criterion involves rational approximation.

Proposition 1.1. *Let ϑ be a real number. The following conditions are equivalent*
(i) *ϑ is irrational.*
(ii) *For any $\epsilon > 0$ there exists $p/q \in \mathbb{Q}$ such that*

$$0 < \left|\vartheta - \frac{p}{q}\right| < \frac{\epsilon}{q}\cdot$$

(iii) *There exist infinitely many $p/q \in \mathbb{Q}$ such that*

$$0 < \left|\vartheta - \frac{p}{q}\right| < \frac{1}{q^2}\cdot$$

(iv) *For any real number $Q > 1$ there exists an integer q in the range $1 \leq q < Q$ and a rational integer p such that*

$$0 < \left|\vartheta - \frac{p}{q}\right| < \frac{1}{qQ}\cdot$$

The most useful implication is an easy one: (ii)⇒(i). *If ϑ is a rational number, there is a positive constant $c = c(\vartheta)$ such that, for any rational number p/q with $p/q \neq \vartheta$,*

$$\left|\vartheta - \frac{p}{q}\right| \geq \frac{c}{q}\cdot$$

Indeed, if $\vartheta = a/b$, then an admissible value for c is $1/b$. This implication (ii)⇒(i) is the most efficient method so far to prove the irrationality of a number. It is a kind of paradox that the easiest implication is at the same time the most useful one. To prove that a number is irrational, it suffices to check (ii), namely to prove that there exist rational approximation in ϵ/q, but in fact there exists much better approximation, in $1/q^2$, as shown by (iii).

The implications (iv)⇒(iii)⇒ (ii)⇒(i) in the irrationality criterion 1.1 are easy. It only remains to prove (i)⇒(iv), which we are going to prove using the *box principle* or *pigeon hole principle*, introduced by Dirichlet in this context.

Proof of (i)⇒(iv). Let $Q > 1$ be given. Define $N = \lceil Q \rceil$: this means that N is the integer such that $N - 1 < Q \le N$. Since $Q > 1$, we have $N \ge 2$.

For $x \in \mathbb{R}$ write $x = \lfloor x \rfloor + \{x\}$ with $\lfloor x \rfloor \in \mathbb{Z}$ (integral part of x) and $0 \le \{x\} < 1$ (fractional part of x). Let $\vartheta \in \mathbb{R} \setminus \mathbb{Q}$. Consider the subset E of the unit interval $[0, 1]$ which consists of the $N + 1$ elements

$$0,\ \{\vartheta\},\ \{2\vartheta\},\ \{3\vartheta\},\ \dots, \{(N-1)\vartheta\},\ 1.$$

Since ϑ is irrational, these $N+1$ elements are pairwise distinct. Split the interval $[0, 1]$ into N intervals

$$I_j = \left[\frac{j}{N}, \frac{j+1}{N}\right] \quad (0 \le j \le N-1).$$

One at least of these N intervals, say I_{j_0}, contains at least two elements of E. Apart from 0 and 1, all elements $\{q\vartheta\}$ in E with $1 \le q \le N - 1$ are irrational, hence belong to the union of the *open* intervals $(j/N,\ (j + 1)/N)$ with $0 \le j \le N - 1$.

If $j_0 = N - 1$, then the interval

$$I_{j_0} = I_{N-1} = \left[1 - \frac{1}{N}\ ;\ 1\right]$$

contains 1 as well as another element of E of the form $\{q\vartheta\}$ with $1 \le q \le N-1$. Set $p = \lfloor q\vartheta \rfloor + 1$. Then we have $1 \le q \le N - 1 < Q$ and

$$p - q\vartheta = \lfloor q\vartheta \rfloor + 1 - \lfloor q\vartheta \rfloor - \{q\vartheta\} = 1 - \{q\vartheta\}, \quad \text{hence} \quad 0 < p - q\vartheta < \frac{1}{N} \le \frac{1}{Q}.$$

Otherwise we have $0 \le j_0 \le N - 2$ and I_{j_0} contains two elements $\{q_1\vartheta\}$ and $\{q_2\vartheta\}$ with $0 \le q_1 < q_2 \le N - 1$. Set

$$q = q_2 - q_1, \quad p = \lfloor q_2\vartheta \rfloor - \lfloor q_1\vartheta \rfloor.$$

Then we have $0 < q = q_2 - q_1 \le N - 1 < Q$ and

$$|q\vartheta - p| = |\{q_2\vartheta\} - \{q_1\vartheta\}| < 1/N \le 1/Q.$$

□

There are other proofs of (i)⇒(iii) – for instance one can use Minkowski's Theorem in the geometry of numbers, which is more powerful than Dirichlet's box principle.

Exercise 1. Let $b \geq 2$ be an integer, $(a_n)_{n\geq 0}$ be a bounded sequence of rational integers and $(u_n)_{n\geq 0}$ an increasing sequence of positive integers. Assume

$$\limsup_{n\to\infty}(u_{n+1} - u_n) = \infty.$$

Show that the number

$$\sum_{n\geq 0} a_n b^{-u_n}$$

is irrational if and only if the set $\{n \geq 0\ ;\ a_n \neq 0\}$ is infinite.

Exercise 2. This exercise extends the irrationality criterion by replacing $\mathbb{Q}$ by $\mathbb{Q}(i)$. The elements in $\mathbb{Q}(i)$ are called the *Gaussian numbers*, the elements in $\mathbb{Z}(i)$ are called the *Gaussian integers*. The elements of $\mathbb{Q}(i)$ will be written p/q with $p \in \mathbb{Z}[i]$ and $q \in \mathbb{Z}$, $q > 0$.

Let ϑ be a complex number. Check that the following conditions are equivalent:
(i) $\vartheta \notin \mathbb{Q}(i)$.
(ii) For any $\epsilon > 0$ there exists $p/q \in \mathbb{Q}(i)$ such that

$$0 < \left|\vartheta - \frac{p}{q}\right| < \frac{\epsilon}{q}\cdot$$

(iii) There exist infinitely many Gaussian numbers $p/q \in \mathbb{Q}(i)$ such that

$$\left|\vartheta - \frac{p}{q}\right| < \frac{\sqrt{2}}{q^{3/2}}\cdot$$

(iv) For any rational integer $N \geq 1$ there exists a rational integer q in the range $1 \leq q \leq N^2$ and a Gaussian integer p such that

$$0 < \left|\vartheta - \frac{p}{q}\right| < \frac{\sqrt{2}}{qN}\cdot$$

Exercise 3. *Let $\vartheta_1, \ldots, \vartheta_m$ be real numbers. Prove that the following conditions are equivalent*
(i) *One at least of $\vartheta_1, \ldots, \vartheta_m$ is irrational.*
(ii) *For any $\epsilon > 0$ there exist $p_1, \ldots, p_m, q$ in $\mathbb{Z}$ with $q > 0$ such that*

$$0 < \max_{1\leq i\leq m}\left|\vartheta_i - \frac{p_i}{q}\right| < \frac{\epsilon}{q}\cdot$$

(iii) *There is an infinite set of $q \in \mathbb{Z}$, $q > 0$, for which there there exist $p_1, \ldots, p_m$ in $\mathbb{Z}$ satisfying*

$$0 < \max_{1\leq i\leq m}\left|\vartheta_i - \frac{p_i}{q}\right| < \frac{1}{q^{1+1/m}}\cdot$$

(iv) *For any integer $Q > 1$ there exists $p_1, \ldots, p_m, q$ in $\mathbb{Z}$ such that $1 \leq q \leq Q^m$ and*

$$0 < \max_{1\leq i\leq m}\left|\vartheta_i - \frac{p_i}{q}\right| \leq \frac{1}{qQ}\cdot$$

A refined version of the irrationality criterion is due to Adolf Hurwitz (1891). One can prove it using either continued fractions or Farey sequences. We do not give a proof here.

Lemma 1.2. *Let ϑ be a real number. The following conditions are equivalent*
(i) *ϑ is irrational.*
(ii) *There exist infinitely many $p/q \in \mathbb{Q}$ such that*

$$0 < \left| \vartheta - \frac{p}{q} \right| \leq \frac{1}{\sqrt{5}q^2}\cdot$$

Of course the implication (ii)⇒(i) in Lemma 1.2 is weaker than the implication (iii)⇒(i) in the irrationality criterion 1.1. What is new is the converse, and the estimate in (ii) with $\sqrt{5}$ is optimal (see §2.1).

1.2 A transcendence criterion

There are (at least) two was of generalizing the irrationality criterion 1.1 into a criterion for transcendence. Instead of considering rational approximations p/q, one may consider algebraic approximations - for such a statement we refer to [GL326, Theorem 15.6]. Here we consider another approach: instead of considering only polynomials of degree 1, namely $qX - p$, we allow polynomials of any degree.

We denote by $\mathrm{H}(f)$ the *naive* (or *usual*) height of a polynomial $f \in \mathbb{C}[X_1, X_2, \ldots, X_n]$, that is the maximum of the moduli of the coefficients, and by $\mathrm{L}(f)$ the length of f, that is the sum of the moduli of the coefficients.

Proposition 1.3. *Let ϑ be a complex numbers. The following conditions are equivalent.*
(i) *ϑ is transcendental.*
(ii) *For any $\kappa > 0$ there exists a polynomial $f \in \mathbb{Z}[X]$ and a positive integer T with*

$$\deg f + \log \mathrm{H}(f) \leq T$$

and

$$0 < |f(\vartheta)| \leq \mathrm{e}^{-\kappa T}.$$

(iii) *For any positive real number $c < \frac{1}{2}$, there exists a positive number T_0 such that, for any $T \geq T_0$, there exists a nonzero polynomial $f \in \mathbb{Z}[X]$ of degree at most T and naive height at most e^T, satisfying $0 < |f(\vartheta)| \leq \mathrm{e}^{-cT^2}$.*
(iv) *For any $H \geq 1$ and $D \geq 1$ there exists a polynomial $f \in \mathbb{Z}[X]$ of degree $\leq D$ and naive height $\mathrm{H}(f) \leq H$ such that*

$$0 < |f(\vartheta)| \leq \sqrt{2}(1 + |\vartheta|)^D H^{-(D-1)/2}.$$

The proofs of (iv)⇒(iii)⇒ (ii) in the transcendence criterion 1.3 are trivial. The proof of (i)⇒(iv) rests on Dirichlet's box principle (see for instance [[GL326, Proposition 15.2]]). The useful part of Proposition 1.3 is (ii)⇒(i), which is equivalent to the following statement:

Corollary 1.4. *Given an algebraic number γ, there exists a positive constant $c = c(\gamma)$ which satisfies the following property.*
Let $f \in \mathbb{Z}[X]$ and T be a positive number such that the the degree of f is at most T and the naive height of f is at most e^T. If $f(\gamma) \neq 0$, then

$$|f(\gamma)| \geq \mathrm{e}^{-cT}.$$

While the irrationality criterion 1.1 is directly used for irrationality proofs, one main tool in transcendence proofs is not really the transcendence criterion 1.3, but rather explicit versions of Corollary 1.4, that we are going to discuss in §2.

The proof of Corollary 1.4 will involve the next auxiliary result: in order to prove a lower bound for a nonzero algebraic number, it suffices to prove an upper bound for its height.

Lemma 1.5. *If $\alpha \in \mathbb{C}^\times$ is a nonzero algebraic number which is root of a polynomial with rational integer coefficients, the absolute values of which are bounded above by some number H, then*

$$|\alpha| \geq \frac{1}{1+H}\cdot$$

In the statement of Lemma 1.5 the polynomial f needs not be the minimal polynomial of α — this remark will be useful.

Proof. We first prove that if α is a complex number which is root of a nonzero polynomial $f(X) = a_0X^n + \cdots + a_n \in \mathbb{Z}[X]$ of degree n with $\max_{0\leq i\leq n} |a_i| \leq H$, then $|\alpha| \leq H+1$. Indeed, this estimate holds trivially if $|\alpha| \leq 1$, while if $|\alpha| > 1$, then

$$\begin{aligned}|\alpha| \leq |a_0\alpha| &= |a_1 + a_2\alpha^{-1} + \cdots + a_n\alpha^{-n+1}|\\ &\leq H\bigl(1 + |\alpha|^{-1} + \cdots + |\alpha|^{-n+1}\bigr) < H\bigl(1 - |\alpha|^{-1}\bigr)^{-1}.\end{aligned}$$

Lemma 1.5 follows by applying this estimate to α^{-1}, which is a root of the polynomial $X^nf(1/X)$. □

When α is an algebraic number, we denote by $\mathrm{H}(\alpha)$ the naive height of the minimal polynomial of α. From Lemma 1.5 one deduces that, if α is an algebraic number, then $|\alpha| \leq \mathrm{H}(\alpha) + 1$. Further, if α is a nonzero algebraic number, then

$$|\alpha| \geq \frac{1}{\mathrm{H}(\alpha)+1}\cdot$$

Proof of Corollary 1.4. From the Theorem on symmetric polynomials, we deduce the following. Let $\gamma \in \mathbb{C}$ be root of a polynomial in $\mathbb{Z}[\ X]$ of degree d, leading coefficient a_0, and complex roots γ_j $(1 \leq j \leq d)$. Let $f \in \mathbb{Z}[X]$ be a polynomial with integer coefficients of degree at most T and naive height at most e^T. Then the polynomial

$$F(X) = a_0^{dL} \prod_{j=1}^{d} \bigl(X - f(\gamma_j)\bigr)$$

has coefficients in $\mathbb{Z}$, its degree is at most $c'T$ and it height at most $\mathrm{e}^{c'T}$, for some constant c' depending only on γ.

Corollary 1.4 follows from Lemma 1.5. □

Exercise 4. *Let $\underline{\vartheta} = (\vartheta_1, \dots, \vartheta_m)$ be a m-tuple of complex numbers. Prove that the following assertions are equivalent.*
(i) *One at least of the numbers $\vartheta_1, \dots, \vartheta_m$ is transcendental, that is*

$$\mathrm{trdeg}_{\mathbb{Q}} \mathbb{Q}(\underline{\vartheta}) \geq 1.$$

(ii) *For any $\kappa > 0$ there exist a positive integer T and a polynomial $f \in \mathbb{Z}[X_1, \dots, X_m]$ such that $\deg f \leq T$, $\mathrm{H}(f) \leq \mathrm{e}^T$ and*

$$0 < |f(\underline{\vartheta})| \leq \mathrm{e}^{-\kappa T}.$$

(iii) *For any $\kappa < 1/2$ there exists a positive integer T_0 such that, for any $T \geq T_0$ there is a polynomial $f \in \mathbb{Z}[X_1, \dots, X_m]$ satisfying $\deg f \leq T$, $\mathrm{H}(f) \leq \mathrm{e}^T$ and*

$$0 < |f(\underline{\vartheta})| \leq \mathrm{e}^{-\kappa T^2}.$$

(iv) *For any $H \geq 1$ and $D \geq 1$ there exists a polynomial $f \in \mathbb{Z}[X_1, \dots, X_m]$ of total degree $\leq D$ and naive height $\mathrm{H}(f) \leq H$ such that*

$$0 < |f(\underline{\vartheta})| \leq \sqrt{2}(1 + |\underline{\vartheta}|)^D H^{-(D-1)/2}.$$

In transcendence proofs one needs explicit versions of Corollary 1.4 and its generalisation in Exercise 4. A very useful tool is provided by the notion of height which is a main character in Diophantine geometry. We introduce it in the next course.

1.3 Criteria for linear independence, for algebraic independence

The irrationality criterion 1.1 and the transcendence criterion 1.3 are the first items of a vast subject which includes also criteria for linear independence and criteria for algebraic independence. A reference is [GL326].

References

[GL326] M. Waldschmidt, *Diophantine approximation on linear algebraic groups. Transcendence properties of the exponential function in several variables.* Grundlehren der Mathematischen Wissenschaften. 326. Berlin: Springer, 2000.
http://dx.doi.org/10.1007/978-3-662-11569-5

Update: 26/04/2021

April 12 - 23, 2021: Hanoi (Vietnam) (online)
CIMPA School on Functional Equations: Theory, Practice and Interaction.

Introduction to transcendental numbers
Michel Waldschmidt

2 Liouville type estimates

2.1 Liouville inequality

We start with an asymptotic version.

Lemma 2.1. *Let α be a real algebraic number of degree $d \geq 2$ and minimal polynomial $P \in \mathbb{Z}[X]$. Define $c = |P'(\alpha)|$. Let $\epsilon > 0$. Then there exists an integer q_0 such that, for any $p/q \in \mathbb{Q}$ with $q \geq q_0$,*

$$\left|\alpha - \frac{p}{q}\right| \geq \frac{1}{(c+\epsilon)q^d}\cdot$$

Proof. Let q be a sufficiently large positive integer and let p be the nearest integer to α. In particular

$$|q\alpha - p| \leq \frac{1}{2}\cdot$$

Denote a_0 the leading coefficient of P and by $\alpha_1, \dots, \alpha_d$ its the roots with $\alpha_1 = \alpha$. Hence

$$P(X) = a_0(X-\alpha_1)(X-\alpha_2)\cdots(X-\alpha_d)$$

and

$$q^d P(p/q) = a_0 q^d \prod_{i=1}^d \left(\frac{p}{q} - \alpha_i\right). \tag{2.2}$$

Also

$$P'(\alpha) = a_0 \prod_{i=2}^d (\alpha - \alpha_i).$$

The left hand side of (2.2) is a rational integer. It is not zero because P is irreducible of degree ≥ 2. For $i \geq 2$ we use the estimate

$$\left|\alpha_i - \frac{p}{q}\right| \leq |\alpha_i - \alpha| + \frac{1}{2q}\cdot$$

We deduce

$$1 \leq q^d a_0 \left|\alpha - \frac{p}{q}\right| \prod_{i=2}^d (|\alpha_i - \alpha| + \frac{1}{2q}).$$

For sufficiently large q the right hand side is bounded from above by

$$q^d \left|\alpha - \frac{p}{q}\right| (|P'(\alpha)| + \epsilon).$$

$\square$

If α is a real root of a quadratic polynomial $P(X) = aX^2 + bX + c$, then $P'(\alpha) = 2a\alpha + b$ is a square root of the discriminant of P. So Hurwitz Lemma 1.2 is optimal for all quadratic numbers having a minimal polynomial of discriminant 5. Incidentally, this shows that 5 is the smallest positive discriminant of an irreducible quadratic polynomial in $\mathbb{Z}[X]$ (of course it is easily checked directly that if a, b, c are three rational integers with $a > 0$ and $b^2 - 4ac$ positive and not a perfect square in $\mathbb{Z}$, then $b^2 - 4ac \geq 5$).

It follows that for the numbers of the form $(a\Phi + b)/(c\Phi + d)$ with integers a, b, c, d having $ad - bc = \pm 1$, one cannot replace in Lemma 1.2 the number $\sqrt{5}$ by a larger number.

On the other hand, Hurwitz Lemma 1.2 shows that Lemma 2.1 is sometimes optimal. This optimality will be one of the main topics of this lecture.

Exercise 5. Prove the nonasymptotic version of Liouville's Theorem as follows. Let α be a real algebraic number of degree $d \geq 2$ and minimal polynomial $P \in \mathbb{Z}[X]$. Then there exists a positive constant $\kappa = \kappa(\alpha)$ such that, for any $p/q \in \mathbb{Q}$ with $q \geq 1$,

$$\left|\alpha - \frac{p}{q}\right| \geq \frac{1}{\kappa q^d}\cdot$$

(a) Prove this result with κ given by

$$\kappa = \max\bigl\{1\ ;\ \max_{|t-\alpha|\leq 1} |P'(t)|\bigr\}.$$

(b) Check also that the same estimate is true with κ given by

$$\kappa = a_0 \prod_{i=2}^{d} (|\alpha_j - \alpha| + 1),$$

where a_0 is the leading coefficient and $\alpha_1, \ldots, \alpha_d$ the roots of P with $\alpha_1 = \alpha$:

$$P(X) = a_0(X - \alpha_1)(X - \alpha_2)\cdots(X - \alpha_d).$$

`Hint:` *For both parts of this exercise, one may distinguish two cases, whether $|\alpha - (p/q)|$ is ≥ 1 or < 1.*

Definition. *A real number ϑ is a* Liouville number *if for any $\kappa > 0$ there exists $p/q \in \mathbb{Q}$ with $q \geq 2$ and*

$$0 < \left|\vartheta - \frac{p}{q}\right| \leq \frac{1}{q^\kappa}\cdot$$

It follows from Lemma 2.1 that Liouville numbers are transcendental. In dynamical systems, an irrational real number *satisfies a Diophantine condition* if is not Liouville: this means that there exists a constant $\kappa > 0$ such that, for any $p/q \in \mathbb{Q}$ with sufficiently large q,

$$\left| \alpha - \frac{p}{q} \right| > \frac{1}{q^\kappa}\cdot$$

Let $b \geq 2$ be an integer. Let us check that the number

$$\vartheta_b = \sum_{n \geq 0} b^{-n!}$$

is a Liouville number. Let $\kappa > 0$ be a real number. For sufficiently large N, set

$$q = b^{N!}, \quad p = \sum_{n=0}^{N} b^{N!-n!}.$$

Then we have

$$0 < \vartheta_b - \frac{p}{q} = \sum_{k \geq 1} \frac{1}{b^{(N+k)!-N!}}\cdot$$

For $k \geq 1$ we use the crude estimate

$$(N+k)! - N! \geq N!N(N+1)\cdots(N+k-1) \geq N!N(k-1)!,$$

which yields

$$0 < \vartheta_b - \frac{p}{q} \leq \frac{2}{q^N}\cdot$$

Exercise 6. Let $(a_n)_{n\geq 0}$ be a bounded sequence of rational integers and $(u_n)_{n \geq 0}$ be an increasing sequence of integers satisfying

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

Assume that the set $\{n \geq 0 \; ; \; a_n \neq 0\}$ is infinite.

Define

$$\vartheta = \sum_{n \geq 0} a_n 2^{-u_n}.$$

Show that ϑ is a Liouville number.

2.2 Heights

There are several definitions of heights for algebraic numbers. For each of them, the set of algebraic numbers of bounded degree and height is a finite set. They play an important role in Diophantine geometry. The most useful one is the absolute logarithmic height.

We first introduce Mahler's measure of a polynomial, and of an algebraic number.

Lemma 2.3. *Let $f \in \mathbb{C}[X]$ be a nonzero polynomial of degree d:*

$$f(X) = a_0X^d + a_1X^{d-1} + \cdots + a_{d-1}X + a_d = a_0\prod_{i=1}^{d}(X - \alpha_i).$$

Then

$$|a_0|\prod_{i=1}^{d}\max\{1, |\alpha_i|\} = \exp\left(\int_0^1 \log|f(\mathrm{e}^{2i\pi t})|dt\right).$$

This is a special case of Jensen's formula for analytic functions. Since both sides of the conclusion of Lemma 2.3 are multiplicative functions of f, it is sufficient to consider the case where f is either a_0 or else $X - \alpha$. In the first case the left hand side is $|a_0|$ and the desired equality plainly holds. In the latter case, the left hand side is $\max\{1, |\alpha|\}$. Therefore Lemma 2.3 is equivalent to the fact that, for any complex number α,

$$\int_0^1 \log|\mathrm{e}^{2i\pi t} - \alpha|dt = \log\max\{1, |\alpha|\}.$$

Under the notation of Lemma 2.3, we define *Mahler's measure* of f by

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

This is a multiplicative function:

$$\mathrm{M}(f_1f_2) = \mathrm{M}(f_1)\mathrm{M}(f_2)$$

for f_1 and f_2 in $\mathbb{C}[X]$, a fact which follows immediately from the definition of M.

When α is an algebraic number with minimal polynomial $f \in \mathbb{Z}[X]$ over $\mathbb{Z}$, we define its *Mahler's measure* by $\mathrm{M}(\alpha) = \mathrm{M}(f)$.

For an algebraic complex number α of degree d, we define the *absolute logarithmic height* of α as

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

Lemma 2.3 gives two equivalent definitions of the absolute logarithmic height of an algebraic number α. There is a third one, which is often the most useful, which involves the archimedean and ultrametric places of the field $\mathbb{Q}(\alpha)$. We refere to [GL326, Chap. 3].

The *house* of an algebraic number is the maximum of the modulus of its conjugates in $\mathbb{C}$:

$$\lceil\overline{\alpha}\rceil = \max\{|\alpha_1|, \ldots, |\alpha_d|\}$$

when the minimal polynomial of α is written in $\mathbb{C}[X]$ as

$$f(X) = a_0X^d + \cdots + a_d = a_0\prod_{i=1}^{d}(X - \alpha_i).$$

The *denominator* $\operatorname{den}(\alpha)$ of α is the positive generator of the ideal of $D \in \mathbb{Z}$ for which $D\alpha$ is an algebraic integer. It is a divisor of a_0.

Among several notions of *size* of an algebraic number, one of the most frequently used is

$$s(\alpha) = \log \max\{\operatorname{den}(\alpha)\,;\, \overline{|\alpha|}\}.$$

Lemma 2.4. *For $\alpha \in \overline{\mathbb{Q}}$ of degree d, we have*

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

and

$$\frac{1}{d}s(\alpha) \le \mathrm{h}(\alpha) \le \log \operatorname{den}(\alpha) + \log\max\bigl\{1, \overline{|\alpha|}\bigr\} \le 2s(\alpha).$$

Proof. The first part of the conclusion can be written

$$2^{-d}\mathrm{H}(\alpha) \le \mathrm{M}(\alpha) \le \mathrm{H}(\alpha)\sqrt{d+1}.$$

The left inequality follows from the identity which relates the coefficients of a polynomial with the roots of this polynomial:

$$a_j = (-1)^j a_0 \sum_{1 \le s_1 < \cdots < s_j \le d} \alpha_{s_1}\cdots\alpha_{s_j}, \qquad (1 \le j \le d).$$

The number of terms in the sum is $\binom{d}{j} \le 2^d$, and each of these terms is bounded from above by $\mathrm{M}(\alpha)/a_0$.

The right inequality follows from the arithmetico-geometric inequality:

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

Using this bound for f^p, with p positive real, we deduce

$$\mathrm{M}(f) \le \left(\int_0^1 \bigl|f\bigl(\mathrm{e}^{2i\pi t}\bigr)\bigr|^p dt\right)^{1/p}.$$

For $p = 2$ we obtain the desired estimate.

The proof of the second series of inequalities does not involve any difficulty and is left as an exercise. □

2.3 Explicit Liouville estimates

Here is an explicit lower bound for the value of a polynomial at an algebraic point, involving the absolute logarithm height $\mathrm{h}(\alpha)$ of an algebraic number α.

> *Let $f \in \mathbb{Z}[X]$ be a polynomial of degree at most N. Let $\gamma \in \mathbb{C}$ be an algebraic number of degree at most d which is not a root of f. Then*
>
> $$|f(\gamma)| \ge \mathrm{L}(f)^{1-d}\mathrm{e}^{-dN\mathrm{h}(\gamma)}.$$

The next result is a generalisation to several variables.

Proposition 2.5 (Liouville's inequality)**.** *Let K be a number field of degree D. Let $\gamma_1, \dots, \gamma_\ell$ be elements of K. Further, let $f \in \mathbb{Z}[X_1, \dots, X_\ell]$ be a polynomial in ℓ variables, with coefficients in $\mathbb{Z}$, which does not vanish at the point $\underline{\gamma} = \big(\gamma_i\big)_{1 \le i \le \ell}$. Assume f is of degree at most N_i with respect to X_i. Then*

$$\log |f(\underline{\gamma})| \geq -(D-1) \log \mathrm{L}(f) - D \sum_{i=1}^{\ell} N_i \mathrm{h}(\gamma_i).$$

Update: 26/04/2021

April 12 - 23, 2021: Hanoi (Vietnam) (online)
CIMPA School on Functional Equations: Theory, Practice and Interaction.

Introduction to transcendental numbers
Michel Waldschmidt

3 Thue Siegel Roth

Let α be an irrational algebraic real number of degree $d \geq 2$. Liouville inequality states that there exists a constant $c = c(\alpha) > 0$ (explicit) such that

$$\left|\alpha - \frac{p}{q}\right| > \frac{c}{q^d}\cdot$$

for all $p/q \in \mathbb{Q}$. Dirichlet's box principle states that there exist infinitely many $p/q \in \mathbb{Q}$ with

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}\cdot$$

For $d = 2$ (α a quadratic irrational real number) we see that both estimates are sharp. This is no longer true for $d \geq 3$. We discuss here improvements of Liouville's inequality; these improvements are deep, we will not give proofs. They play an important role in Diophantine geometry.

Liouville's estimate for the rational Diophantine approximation of $\sqrt[3]{2}$ is

$$\left|\sqrt[3]{2} - \frac{p}{q}\right| > \frac{1}{5q^3}$$

for sufficiently large q (use Lemma 2.1 with $P(X) = X^3 - 2$, $c = 3\sqrt[3]{4} < 5$). Thue was the first to achieve an improvement of the exponent 3: for the case of cubic real numbers he replaced the exponent 3 of Liouville with $\frac{5}{2} + \epsilon$ for all $\epsilon > 0$ (and the constant c depends on α and ϵ, but the constant c is not effective, an admissible valuer cannot be computed using Thue's proof). A explicit estimate was then obtained by A. Baker in 1964:

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

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

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

From his result, Thue deduced that *for any fixed $k \in \mathbb{Z} \setminus \{0\}$, there are only finitely many $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ satisfying the Diophantine equation $x^3 - 2y^3 = k$.*

The result of Baker shows more precisely that if $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ is a solution to $x^3 - 2y^3 = k$, then

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

M. Bennett gave the sharper estimate: *for any $(x, y) \in \mathbb{Z}^2$ 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 3.1. *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 $p/q \in \mathbb{Q}$ with $q > 0$,*

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

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

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

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 $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ have $(x, y) \neq (0, 0)$. 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 (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. From

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

using (ii), we deduce

$$c_2 p^{3-\eta} \le c_9 q^3 \left| \alpha - \frac{p}{q} \right|,$$

and (i) easily follows.

□

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 $q \ge q_0$,*

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

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.

If κ is an irrationality exponent for ϑ, then any number $> \kappa$ is also an irrationality exponent for ϑ. From Proposition 1.1, it follows that any irrationality exponent κ satisfies $\kappa \ge 2$. Irrational quadratic numbers have irrationality exponent 2. It is known 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.*

An important chapter in Diophantine approximation is the metric theory which studies the properties which are satisfied by almost all (real or complex) numbers for Lebesgue measure. We only quote the following result: *for almost all real numbers ϑ, any $\kappa > 2$ is an irrationality exponent for ϑ.*

From Liouville's inequality in Lemma 2.1 it follows that any irrational algebraic real number α has a finite irrationality exponent $\le d$. Liouville numbers are by definition exactly the irrational real numbers which have no finite irrationality exponent.

For any $\kappa \ge 2$, 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 are

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

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

The fact that any irrational algebraic real number of degree $d \geq 3$ has an irrationality exponent is $< d$ has very important corollaries in the theory of Diophantine equations.

Theorem 3.3 (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 3.3 is called *Thue equation*. The connexion between Thue equation and Liouville's inequality has been explained in Lemma 3.1 in the special case $\sqrt[3]{2}$; the general case is similar.

Lemma 3.4. *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 3.2 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 $j = \lfloor \sqrt{d} \rfloor$ it follows that $2\sqrt{d}$ is an irrationality exponent for α. Siegel's generalization of Thue's result played an essential role in his proof[1] in 1929 that there are only finitely many integer points on a curve of genus ≥ 1.

Dyson and Gel'fond in 1947 independently refined Siegel's estimate and replaced the hypothesis in Thue's Theorem 3.2 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 3.5 (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.*

An equivalent statement is :

> *For any real algebraic number α and for any $\epsilon > 0$, there exists $q_0 > 0$ such that, for $p/q \in \mathbb{Q}$ with $q \geq q_0$, we have $|\alpha - p/q| > q^{-2-\epsilon}$.*

[1] U. Zannier (ed.), *On some applications of Diophantine approximations*, a translation of Carl Ludwig Siegel's *Über einige Anwendungen diophantischer Approximationen* by Clemens Fuchs. Edizioni Della Normale, Quaderni Monographs 2, 2014.

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, the sequence of partial quotients of which is not bounded!

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

$$\vartheta = \sum_{n\geq 0} b^{-u_n} \tag{3.6}$$

This number is rational if and only if its sequence of digits in basis b is ultimately periodic, which is the case when $(u_n)_{n\geq 0}$ is ultimately an arithmetic progression.

Assume that ϑ is irrational. A conjecture of Borel (1950) states that *the digits in the expansion in a basis $b \geq 2$ of a real algebraic irrational number should all occur with the same frequency.* For $b \geq 3$, the expansion in basis b of the number (3.6) has no digit 2, hence Borel predicts that it is transcendental. For $b = 2$, if the sequence of 1's in the binary expansion of a number ϑ is lacunary, then, again, Borel predicts that ϑ is transcendental. We are very far from such results.

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

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

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

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

then ϑ is a Liouville number, and therefore is transcendental. For instance the sequence $u_n = n!$ satisfies this condition: hence the number $\vartheta_b = \sum_{n\geq 0} b^{-n!}$ is transcendental (see § 2.1).

Roth's Theorem 3.5 yields the transcendence of the number ϑ in (3.6) under the weaker hypothesis

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

The sequence $u_n = \lfloor 2^{\kappa n} \rfloor$ satisfies this condition as soon as $\kappa > 1$. For example with $\kappa = \frac{\log 3}{\log 2}$ the transcendence of the number

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

follows from Theorem 3.5.

A stronger result follows from Ridout's Theorem 4.3 below, using the fact that the denominators b^{u_n} are powers of b.

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

The set of S–integers is the subring of $\mathbb{Q}$ generated by the elements $1/p$ with $p \in S$. We denote it by $S^{-1}\mathbb{Z}$. The group of units of $S^{-1}\mathbb{Z}$ is a multiplicative subgroup $(S^{-1}\mathbb{Z})^\times$ of $\mathbb{Q}^\times$, its elements are the *S–units*. If $S = \{p_1, \ldots, p_s\}$, then

$$(S^{-1}\mathbb{Z})^\times = \left\{ p_1^{k_1} \cdots p_s^{k_s} \;\mid\; (k_1, \ldots, k_s) \in \mathbb{Z}^s \right\} \subset \mathbb{Q}^\times$$

and

$$S^{-1}\mathbb{Z} = \left\{ \frac{a}{b} \;\mid\; a \in \mathbb{Z},\; b \in (S^{-1}\mathbb{Z})^\times \right\} \subset \mathbb{Q}.$$

Here is a result due to Ridout (1957) (see Corollary 4.4 below).

> *Let S be a finite set of prime numbers. Let α be a real algebraic number. For any $\epsilon > 0$, the set of S–integers a/b such that*
>
> $$\left| \alpha - \frac{a}{b} \right| < \frac{1}{b^{1+\epsilon}}$$
>
> *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 (3.6). 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.

Update: 26/04/2021

April 12 - 23, 2021: Hanoi (Vietnam) (online)
CIMPA School on Functional Equations: Theory, Practice and Interaction.

Introduction to transcendental numbers
Michel Waldschmidt

4 Schmidt's Subspace Theorem

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.

The Subspace Theorem is one of the most powerful tools in Diophantine geometry; it is a kind of paradox that for transcendence proofs, one does not know how to replace the Liouville type estimates of §2.3 by stronger versions arising from the Thue–Siegel–Roth–Schmidt theory.

For $\mathbf{x} = (x_1, \dots, x_n) \in \mathbb{Z}^n$, define $|\mathbf{x}| = \max\{|x_1|, \dots, |x_n|\}$.

Theorem 4.1 (Schmidt Subspace Theorem)**.** *For $n \geq 2$ let $L_1, \dots, L_n$ be independent linear forms in n variables with algebraic coefficients. Let $\epsilon > 0$. Then the set*

$$\{\mathbf{x} = (x_1, \dots, x_n) \in \mathbb{Z}^n \ ; \ |L_1(\mathbf{x}) \cdots L_n(\mathbf{x})| \leq |\mathbf{x}|^{-\epsilon}\}$$

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

We deduce the Thue–Siegel–Roth's Theorem 3.5 from Theorem 4.1 as follows. Let α be a real irrational algebraic number and let $\epsilon > 0$. Consider the set

$$E_\epsilon = \left\{ (q,p) \in \mathbb{Z}^2 \ \mid \ q|\alpha q - p| < \frac{1}{q^\epsilon} \right\}.$$

Use Theorem 4.1 with

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

Theorem 4.1 says that the set E_ϵ is contained in the union of finitely many proper subspaces of $\mathbb{Q}^2$. A $\mathbb{Q}$-vector subspace of $\mathbb{Q}^2$ which is not $\{0\}$ not $\mathbb{Q}^2$ (that is *a proper subspace*) is 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 the set

$$\left\{ \frac{p}{q} \ \mid \ (q,p) \in E_\epsilon \right\} = \left\{ \frac{p}{q} \ \mid \ q|\alpha q - p| < \frac{1}{q^\epsilon} \right\}$$

is finite.

For x a nonzero rational number, write the decomposition of x into prime factors

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

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

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

The product formula is

$$|x| \prod_p |x|_p = 1$$

for all $x \in \mathbb{Q}^\times$.

For a nonzero rational number x, we have

$$x \in \mathbb{Z} \iff v_p(x) \geq 0 \text{ for all primes } p \iff |x|_p \leq 1 \text{ for all primes } p.$$

Given a finite set S of prime numbers, a nonzero rational number x is an S–integer if and only if $v_p(x) \geq 0$ for all primes $p \notin S$, and x is an S–unit if and only if $v_p(x) = 0$ for all primes $p \notin S$. For an S–unit x, the product formula is

$$|x| \prod_{p \in S} |x|_p = 1.$$

We now state a special case of Schmidt's Subspace Theorem (1972) which includes its p-adic extension by H.P. Schlickewei (1976).

Theorem 4.2 (Schmidt–Schlickewei Subspace Theorem)**.** *Let $n \geq 2$ be a positive integer, S a finite set of prime numbers. Let $L_1, \ldots, L_n$ be n independent linear forms in n variables with algebraic coefficients. Further, for each $p \in S$ let $L_{1,p}, \ldots, L_{n,p}$ be n independent linear forms in n variables with* **rational** *coefficients. Let $\epsilon > 0$. Then the set of $\mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{Z}^n$ such that*

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

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

Here is Ridout's Theorem.

Theorem 4.3 (D. Ridout, 1958)**.** *Let α and β be two algebraic numbers with $(\alpha, \beta) \neq (0,0)$. For $p \in S$, let α_p and β_p be two rational numbers with $(\alpha_p, \beta_p) \neq (0,0)$. Let $\epsilon > 0$. Then the set of rational numbers a/b such that*

$$b|b\alpha - a\beta| \prod_{p \in S} |b\alpha_p - a\beta_p|_p < \frac{1}{\max\{|a|, b\}^\epsilon}$$

is finite.

Corollary 4.4. *Let S be a finite set of prime numbers. Let α be a real algebraic number. For any $\epsilon > 0$, the set of S–integers a/b such that*

$$\left|\alpha - \frac{a}{b}\right| < \frac{1}{b^{1+\epsilon}}$$

is finite.

Corollary 4.4 follows from Theorem 4.3 by taking $\beta = 1$, $\alpha_p = 1$ and $\beta_p = 0$ for $p \in S$.

Ridout's Theorem 4.3 is the special case $n = 2$ of the Subspace Theorem: in Theorem 4.2, take

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

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

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

and

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

since b is an S–unit. As we have seen when we deduced the Thue–Siegel–Roth's Theorem 3.5 from Schmidt Subspace Theorem 4.1, a subset E of $\mathbb{Z}^2$ is contained in a finite union of hyperplanes of $\mathbb{Q}^2$ if and only if the set of $y/x \in \mathbb{Q}$, where (x, y) ranges over the set of elements in E with $x \neq 0$, is finite.

We derive a further consequence, dealing with exponential Diophantine equations, of the special case of the Subspace Theorem 4.2 where the linear forms $L_1, \dots, L_n$ also have rational coefficients. We start with an exercise.

Exercise 7. *Show that the only solutions of the equation $2^a + 3^b = 5^c$ in nonnegative integers a, b and c are given by*

$$2 + 3 = 5, \quad 2^2 + 1 = 5, \quad 2^4 + 3^2 = 5^2.$$

The finiteness of the set of solutions of such an equation is a general fact: we deduce from Ridout's Theorem 4.3 the following statement:

Corollary 4.5. *Let S be a finite set of prime numbers and let $n \geq 2$. Then the set of solutions of the equation $x_1 + x_2 = 1$ in S–units x_1, x_2 is finite.*

The S–unit equation was introduced by C.L. Siegel in his seminal 1929 paper, in the more general context of number fields.

Proof. Let (x_1, x_2) be a solution of the equation $x_1 + x_2 = 1$ in S–units. Let y_0 be the least common denominator of x_1 and x_2. Set $y_1 = y_0 x_1$ and $y_2 = y_0 x_2$.

Then y_0, y_1, y_2 are relatively prime integers, they are S–units, and $y_1 + y_2 = y_0$. Introduce the three linear forms in two variables Y_1, Y_2

$$\Lambda_1(Y_1, Y_2) = Y_1, \quad \Lambda_2(Y_1, Y_2) = Y_2, \quad \Lambda_0(Y_1, Y_2) = Y_1 + Y_2.$$

Notice that $\Lambda_j(y_1, y_2) = y_j$ for $j = 0, 1, 2$, and that any two linear forms among $\Lambda_0, \Lambda_1, \Lambda_2$ are linearly independent. Recall the notation $|\mathbf{y}| = \max\{|y_0|, |y_1|, |y_2|\}$. Let $k \in \{0, 1, 2\}$ be an index such that $|\mathbf{y}| = |y_k|$, and let ℓ, m be the two other indices, so that $\{0, 1, 2\} = \{k, \ell, m\}$.

Since y_0, y_1, y_2 are relatively prime rational integers, for $p \in S$, we have $\max\{|y_0|_p, |y_1|_p, |y_2|_p\} = 1$; let $k_p \in \{0, 1, 2\}$ be an index such that $|y_{k_p}|_p = 1$, and let ℓ_p, m_p be the two other indices, so that $\{0, 1, 2\} = \{k_p, \ell_p, m_p\}$.

Consider the linear forms

$$L_1 = \Lambda_\ell, \quad L_2 = \Lambda_m, \qquad L_{1p} = \Lambda_{\ell_p}, \quad L_{2p} = \Lambda_{m_p} \quad (p \in S).$$

Notice that

$$L_1(y_1, y_2)L_2(y_1, y_2) = y_\ell y_m = \frac{y_0 y_1 y_2}{y_k} = \pm \frac{y_0 y_1 y_2}{|\mathbf{y}|},$$

while

$$L_{1p}(y_1, y_2)L_{2p}(y_1, y_2) = y_{\ell_p} y_{m_p} = \frac{y_0 y_1 y_2}{y_{k_p}}$$

and

$$|L_{1p}(y_1, y_2)L_{2p}(y_1, y_2)|_p = |y_0 y_1 y_2|_p.$$

From the product formula, using the fact that $y_0 y_1 y_2$ is an S unit, one deduces

$$|y_0 y_1 y_2| \prod_{p \in S} |y_0 y_1 y_2|_p = 1.$$

Therefore

$$|L_1(y_1, y_2)L_2(y_1, y_2)| \prod_{p \in S} |L_{1p}(y_1, y_2)L_{2p}(y_1, y_2)|_p = \frac{1}{|\mathbf{y}|}.$$

From Ridout's Theorem 4.3 with $\epsilon = 1$, one deduces that the set of y_1/y_2 is finite. From $y_1 + y_2 = y_0$ we deduce that the sets of y_1/y_0 and y_2/y_0 are finite. Corollary 4.5 follows.

□

It turns out that the result of Corollary 4.5 is effective: one can bound from above the (numerators and denominators of the) solutions x_1 and x_2. The proof rests on transcendence methods and lower bounds for linear combinations of logarithms of algebraic numbers – see Corollary 5.5 in § 5.

We now consider the more general equation

$$X_1 + \cdots + X_n = 1, \tag{4.6}$$

where n is a fixed positive integer and the values $x_1, \dots, x_n$ taken by the unknown $X_1, \dots, X_n$ are S–units in $\mathbb{Q}$ for a fixed given finite set S of prime numbers. This equation has infinitely many solutions as soon as $n \geq 3$ and S is nonempty: for $p \in S$ and $a \in \mathbb{Z}$,

$$x_1 = p^a, \quad x_2 = -p^a, \quad x_3 = 1, \qquad p^a - p^a + 1 = 1.$$

In view of this example, we will say that a solution $(x_1, \dots, x_n) \in ((S^{-1}\mathbb{Z})^\times)^n$ of equation (4.6) is *non degenerate* if no nontrivial subsum vanishes:

$$x_1 + \cdots + x_n = 1$$

and

$$\sum_{i \in I} x_i \neq 0 \quad \text{for any nonempty subset } I \text{ of } \{1, \dots, n\}.$$

Without giving all details, we explain how to deduce, from the Subspace Theorem 4.2, the following statement.

Corollary 4.7. *Let S be a finite set of primes and n a positive integer. Then the set of nondegenerate solutions $(x_1, \dots, x_n) \in ((S^{-1}\mathbb{Z})^\times)^n$ of equation (4.6) is finite.*

Sketch of proof of Corollary 4.7 as a consequence of the Subspace Theorem 4.2. The proof is by induction on n. A first remark is that the statement of Corollary 4.7 is equivalent to the next one (which only looks more general):

> *For any finite set S of primes, any positive integer n and any rational numbers $c_1, \dots, c_n$, the set of $(x_1, \dots, x_n) \in ((S^{-1}\mathbb{Z})^\times)^n$ satisfying*
>
> $$c_1x_1 + \cdots + c_nx_n = 1$$
>
> *and*
>
> $$\sum_{i \in I} c_i x_i \neq 0 \quad \textit{for any nonempty subset } I \textit{ of } \{1, \dots, n\}$$
>
> *is finite.*

This last statement is in fact a consequence of Corollary 4.7: we deduce it by enlarging the set S of primes to a finite set $S' \supset S$, so that $c_1, \dots, c_n$ are S'–units.

In the same vein, by reducing to the same denominator, one can phrase Corollary 4.7 in an equivalent form by stating that the set of $(y_1, \dots, y_{n+1}) \in (\mathbb{Z} \cap (S^{-1}\mathbb{Z})^\times)^{n+1}$, satisfying

$$y_1 + \cdots + y_n = y_{n+1} \quad \text{and} \quad \gcd(y_1, \dots, y_{n+1}) = 1,$$

and

$$\sum_{i \in I} y_i \neq 0 \quad \text{when } I \text{ is a nonempty subset of } \{1, \dots, n\},$$

is finite.

Starting with a solution $\mathbf{y}$ of

$$y_1 + \cdots + y_n = y_{n+1}$$

using the assumption $\gcd(y_1, \ldots, y_{n+1}) = 1$, we consider for each prime $p \in S$ an index $i_p \in \{1, \ldots, n+1\}$ such that $|y_{i_p}|_p = 1$. We also consider an index i_0 such that $|y_{i_0}| = \max_{1 \le i \le n+1} |y_i|$. In other terms $|y_{i_0}| = |\mathbf{y}|$. The tuple $\bigl(i_0, (i_p)_{p \in S}\bigr)$ can take only finitely many possible values – we fix one of them.

We introduce the following $n+1$ linear forms Λ_j $(1 \le j \le n+1)$ in $Y_1, \ldots, Y_n$:

$$\Lambda_j = Y_j \quad \text{for} \quad 1 \le j \le n \quad \text{and} \quad \Lambda_{n+1} = Y_1 + \cdots + Y_n.$$

Clearly, any n distinct linear forms among $\Lambda_1, \ldots, \Lambda_{n+1}$ are linearly independent. We shall use the Subspace Theorem 4.2 with the following linear forms in the variables $Y_1, \ldots, Y_n$:

$$\{L_1, \ldots, L_n\} = \{\Lambda_j \;\mid\; 1 \le j \le n+1,\ j \ne i_0\}$$

and, for any prime p in S,

$$\{L_{1p}, \ldots, L_{np}\} = \{\Lambda_j \;\mid\; 1 \le j \le n+1,\ j \ne i_p\}.$$

We write

$$\prod_{i=1}^{n} |L_i(\mathbf{y})| = \frac{1}{|\mathbf{y}|} \prod_{j=1}^{n+1} |\Lambda_j(\mathbf{y})|$$

and, for each prime $p \in S$,

$$\prod_{i=1}^{n} |L_{ip}(\mathbf{y})|_p = \prod_{j=1}^{n+1} |\Lambda_j(\mathbf{y})|_p.$$

For any prime p not in S and for $j = 1, \ldots, n+1$, we have $|\Lambda_j(\mathbf{y})|_p = 1$. From the product formula

$$|\Lambda_j(\mathbf{y})| \prod_p |\Lambda_j(\mathbf{y})|_p = 1$$

for $1 \le j \le n+1$, we deduce the estimate

$$|L_1(\mathbf{y}) \cdots L_n(\mathbf{y})| \prod_{p \in S} |L_{1p}(\mathbf{y}) \cdots L_{np}(\mathbf{y})|_p = \frac{1}{|\mathbf{y}|},$$

which shows that we can apply Subspace Theorem 4.2 with $\epsilon = 1$.

It follows that the solutions $(y_1, \ldots, y_n)$ we are considering belong to a finite union of proper subspaces of $\mathbb{Z}^n$. We are reduced to consider a finite set of Diophantine equations of the form

$$c_1 Y_1 + \cdots + c_n Y_n = 0,$$

where $c_1,\dots,c_n$ are fixed elements of $\mathbb{Z}$, not all 0. We fix such an equation, we fix an index $j_1 \in \{1,\dots,n\}$ with $c_{j_1} \neq 0$ and we write

$$\sum_{\substack{1\le i\le n\\ i\neq j_1}} \frac{-c_i}{c_{j_1}}\frac{y_i}{y_{j_1}} = 1.$$

We use the preliminary remark of this proof (we enlarge S if necessary so that c_i/c_{j_1} becomes an S–unit for $i=1,\dots,n$). We also select one such subsum which is non degenerate. We deduce from the induction hypothesis that there is an index j_2, $(1\le j_2\le n,\ j_2\neq j_1)$ such that the set of y_{j_2}/y_{j_1} is finite. We now write the initial equation in the form

$$\sum_{\substack{1\le i\le n\\ i\neq j_1, i\neq j_2}} \frac{y_i}{y_{j_1}} - \frac{y_{n+1}}{y_{j_1}} = -1 - \frac{y_{j_2}}{y_{j_1}}\cdot$$

The right hand side is a nonzero constant, since $y_{j_2}+y_{j_1}\neq 0$ (here we use the assumption on nonvanishing subsums for subsums of two terms only). Again, we enlarge S if necessary, so that $-1-y_{j_2}/y_{j_1}$ becomes an S–unit. The left hand side is a sum of $n-1$ terms which are S–units. This sum is non degenerate (no nontrivial subsum vanishes): indeed it follows from the assumption on nonvanishing subsums (here we need the full assumption, not only for subsums of two terms) that no sum of the form

$$\sum_{i\in I} y_i \quad \text{nor} \quad \sum_{i\in I} y_i - y_{n+1} \quad \text{for} \quad \emptyset \neq I \subset \{1,\dots,n\}\setminus\{i_1,\ i_2\}$$

can vanish. We obtain the final conclusion by using the induction hypothesis once more. □

The proof of Corollary 4.7 is noneffective: in general, there is no method (yet) to derive an upper bound for the size of the solutions. But upper bounds for the number of solutions are available. To give an upper bound for the number of subspaces in the conclusion of the Subspace Theorem 4.2 has been an open problem from 1970 to 1980, when it has been solved by W.M. Schmidt.

The general case of the Subspace Theorem [LN1467, Chap. V, Th. 1D] involves a finite set of places of a number field K, containing the places at infinity. One replaces $\mathbf{x}\in\mathbb{Z}^n$ with $\mathbf{x}\in K^n$ with all components algebraic integers in K. One replaces $|\mathbf{x}|^{-\epsilon}$ with $H(\mathbf{x})^{-\epsilon}$, where

$$H(\mathbf{x}) = \prod_{v\in M_K} \max_{1\le i\le n} |x_i|_v,$$

where M_K is the set of places of K. And the linear forms $L_{1,p}$ have coefficients in K instead of $\mathbb{Q}$.

References

[LN1467] W. M. Schmidt, *Diophantine approximations and Diophantine equations*, vol. **1467** of Lecture Notes in Mathematics, Springer-Verlag, Berlin, 1991.

Update: 26/04/2021
April 12 - 23, 2021: Hanoi (Vietnam) (online)
CIMPA School on Functional Equations: Theory, Practice and Interaction.

Introduction to transcendental numbers
Michel Waldschmidt

5 Effective methods

5.1 Linear combinations of logarithms

Let $a_1,\dots,a_n$, $b_1,\dots,b_n$ be rational integers with the a_i's all greater than one. We assume

$$a_1^{b_1}\cdots a_n^{b_n}\neq 1,$$

and we ask for a lower bound for the distance between these two numbers.

There is a trivial estimate: a nonzero rational number is at least as large as the inverse of a denominator:

$$\begin{aligned}\left|a_1^{b_1}\cdots a_n^{b_n}-1\right| &\geq \prod_{b_i<0} a_i^{b_i}\\ &\geq \exp\left\{-\sum_{i=1}^n |b_i|\log a_i\right\}\\ &\geq \exp\bigl\{-nB\log A\bigr\},\end{aligned}$$

where $B=\max\{|b_1|,\dots,|b_n|\}$ and $A=\max\{a_1,\dots,a_n\}$. This kind of estimate extends to algebraic α's. It belongs to the family of Liouville's inequalities § 2.

The dependence in n and A in Liouville's inequality is sharp, but the main interest for applications is with the dependence in B. In order to see what can be expected, it is convenient to give a connection with measures of linear independence of logarithms of algebraic numbers. If

$$0<\left|a_1^{b_1}\cdots a_n^{b_n}-1\right|\leq\frac{1}{2},$$

then

$$\frac{1}{2}\bigl|b_1\log a_1+\cdots+b_n\log a_n\bigr|\leq\left|a_1^{b_1}\cdots a_n^{b_n}-1\right|\leq 2\bigl|b_1\log a_1+\cdots+b_n\log a_n\bigr|$$

Therefore the problem of obtaining a lower bound for the distance between 1 and the product $a_1^{b_1}\cdots a_n^{b_n}$ is equivalent to obtaining a lower bound for the nonzero number $b_1\log a_1+\cdots+b_n\log a_n$.

An easy application of Dirichlet's box principle now yields:

Lemma 5.1. *Let n, $a_1, \dots, a_n$ be rational integers, all of which are at least 2. Define $A = \max\{a_1, \dots, a_n\}$. Then for every integer $B \geq 4 \log A$, there exist rational integers $b_1, \dots, b_n$ with*

$$0 < \max_{1 \leq i \leq n} |b_i| < B$$

such that

$$\left| a_1^{b_1} \cdots a_n^{b_n} - 1 \right| \leq \frac{2n \log A}{B^{n-1}} \cdot$$

If $a_1, \dots, a_n$ are multiplicatively independent, then the left hand side is not zero. The upper bound is polynomial in $1/B$, while Liouville's inequality is exponential in $-B$. We shall see that, as far as the dependence in B is concerned, Lemma 5.1 is closer to the truth than Liouville's lower bound.

It is often (but not always) the case that Dirichlet's box principle is a good guide to know what to expect. Another guide it metrical number theory: for almost all tuples of real numbers $a_1, \dots, a_n$, Dirichlet's box principle is essentially best possible.

In 1935, one year after he had solved the seventh problem of D. Hilbert, A. O. Gel'fond used his transcendence method in order to derive a lower bound for a linear combination of two logarithms of algebraic numbers with algebraic coefficients. Let us give a simple example of such an estimate: for a_1, a_2 multiplicatively independent positive rational integers, and for $\epsilon > 0$, there exists a constant $C_1 = C_1(a_1, a_2, \epsilon)$, which can be explicitly computed, such that, for all $(b_1, b_2) \in \mathbb{Z}^2$ with $(b_1, b_2) \neq (0, 0)$, if we set $B = \max\{|b_1|, |b_2|, 2\}$, then

$$\left| a_1^{b_1} a_2^{b_2} - 1 \right| \geq C_1 \exp\left\{ -(\log B)^{5+\epsilon} \right\}.$$

In 1939, A. O. Gel'fond refined the estimate and replaced the exponent $5 + \epsilon$ by $3 + \epsilon$, and in 1949 he [2] reached $2 + \epsilon$. At the same time he gave an estimate which is valid for any $n \geq 2$:

Theorem 5.2 (Gel'fond's Ineffective Estimate)**.** *Let $(a_1, \dots, a_n)$ be a n-tuple of positive multiplicatively independent rational integers. For every $\delta > 0$, there exists a positive constant $C_2 = C_2(a_1, \dots, a_n, \delta)$ such that, if $b_1, \dots, b_n$ are rational integers, not all of which are zero, and if we set $B = \max\{|b_1|, \dots, |b_n|, 2\}$, then*

$$\left| a_1^{b_1} \cdots a_n^{b_n} - 1 \right| \geq C_2 \mathrm{e}^{-\delta B}.$$

For the proof of Theorem 5.2, A. O. Gel'fond used a result of his own, which was a refinement of earlier results due to A. Thue, C. L. Siegel and F. Dyson (see § 3). See [GL326, Theorem 1.9].

This proof produces a lower bound for $\left| a_1^{b_1} \cdots a_n^{b_n} - 1 \right|$ using a lower bound for $|\alpha - (p/q)|$. By means of similar arguments, one can go backwards and deduce nontrivial measures of rational approximation for algebraic numbers

[2] Explicit estimates were provided in 1968 by A. Schinzel

using measures of linear independence for logarithms of algebraic numbers (see [GL326, § 10.4.1]).

The proof of Theorem 5.2 does not enable one to compute the constant C_2, because one uses the Thue-Siegel-Roth Theorem which is not *effective*.

5.2 Baker's transcendence results

In his book, A. O. Gel'fond emphasized the importance of getting a generalization of this statement to more than two logarithms. Let $\log \alpha_1, \ldots, \log \alpha_n$ be n logarithms of algebraic numbers which are linearly independent over $\mathbb{Q}$. The question is to prove that they are also linearly independent over the field $\overline{\mathbb{Q}}$ of algebraic numbers. For $n = 2$, this is the Theorem of Gel'fond-Schneider. This problem was solved in 1966 by A. Baker.

Theorem 5.3 (Baker)**.** *If* $\log \alpha_1, \ldots, \log \alpha_n$ *are* $\mathbb{Q}$*-linearly independent logarithms of algebraic numbers, then the* $n+1$ *numbers* $1, \log \alpha_1, \ldots, \log \alpha_n$ *are linearly independent over* $\overline{\mathbb{Q}}$*.*

From Baker's Theorem 5.3, one easily deduces that if a number of the form

$$\mathrm{e}^{\beta_0} \alpha_1^{\beta_1} \cdots \alpha_n^{\beta_n} = \exp\{\beta_0 + \beta_1 \log \alpha_1 + \cdots + \beta_n \log \alpha_n\}$$

(with $\beta_i \in \overline{\mathbb{Q}}$, and $\alpha_i \in \overline{\mathbb{Q}}^\times$) is algebraic, then $\beta_0 = 0$, and moreover, either $\log \alpha_1, \ldots, \log \alpha_n$ are all zero, or else the numbers $1, \beta_1, \ldots, \beta_n$ are linearly dependent over $\mathbb{Q}$.

Also Theorem 5.3 shows that any nonzero element in the $\overline{\mathbb{Q}}$-vector space

$$\{\beta_1 \log \alpha_1 + \cdots + \beta_n \log \alpha_n \; ; \; n \geq 0, \; \beta_i \in \overline{\mathbb{Q}}, \; \alpha_i \in \overline{\mathbb{Q}}^\times\}$$

spanned by the logarithms of algebraic numbers is transcendental.

At the same time when he proved these transcendence results, Baker produced effective nontrivial lower bounds for linear combinations of logarithms. The main parameter is the maximum absolute value of the coefficients, B. The best possible estimate was achieved by Feldman in 1968.

Ultrametric analogs were developed (work of Mahler, Coates, van der Poorten, Yu Kunrui). In terms of B, the following best possible estimates have been achieved.

Theorem 5.4. *Let* $a_1, \ldots, a_n$ *be positive multiplicatively independent rational integers and* $b_1, \ldots, b_m$ *rational integers, not all of which are zero; let* $B = \max\{2, |b_1|, \ldots, |b_n|\}$*. Assume*

$$a_1^{b_1} \cdots a_n^{b_n} \neq 1$$

(a)*. There exists a positive effectively computable number* $C_3 = C_3(a_1, \ldots, a_n)$ *such that*

$$\left| a_1^{b_1} \cdots a_n^{b_n} - 1 \right| \geq B^{-C_3}.$$

(b). *Let p be a prime number. There exists a positive effectively computable number $C_4 = C_4(a_1, \ldots, a_n, p)$ such that*

$$\left| a_1^{b_1} \cdots a_n^{b_n} - 1 \right|_p \geq B^{-C_4}.$$

Such estimates are valid more generally when the integers $a_1, \ldots, a_n$ are replaced by algebraic numbers $\alpha_1, \ldots, \alpha_n$.

5.3 The S–unit equation

Here is a corollary to Theorem 5.4, which is an effective version of Corollary 4.5. Let S be a finite set of prime numbers. We consider the so–called *S–unit equation*

$$x + y = z$$

where the unknown x, y, z are S–units. If (x, y, z) is a solution, then for each $p \in S$, (px, py, pz) is a solution, as well as $(p^{-1}x, p^{-1}y, p^{-1}z)$. Therefore it is natural to assume that x, y, z are in $\mathbb{Z}$ and are relatively prime.

Corollary 5.5. *Let $S = \{p_1, \ldots, p_s\}$ be a finite set of prime numbers. Then there exists an effectively computable constant $C_6 = C_6(p_1, \ldots, p_s)$ such that any solution (x, y, z) in $(\mathbb{Z} \cap (S^{-1}\mathbb{Z})^\times)^3$ with $\gcd(x, y, z) = 1$ satisfies*

$$\max\{|x|, |y|, |z|\} \leq C_6.$$

Proof. Let $M = \max\{|x|, |y|, |z|\}$. By symmetry, there is no loss of generality to assume $M = |z|$. Each of x, y, z is of the form $p_1^{k_1} \cdots p_s^{k_s}$, with $k_i \in \mathbb{Z}_{\geq 0}$. Let B be the maximum of these exponents. Clearly,

$$2^B \leq M \leq (p_1 \cdots p_s)^B.$$

Let $p \in S$ be such that $|z|_p < 1$. Since $\gcd(x, y, z) = 1$, we have $|x|_p = |y|_p = 1$. We use part (b) of Theorem 5.4 with $a_1^{b_1} \cdots a_n^{b_n} = -\frac{x}{y}$ which is $\neq 1$:

$$|z|_p = |-x-y|_p = \left| -\frac{x}{y} - 1 \right|_p \geq B^{-C_4}.$$

The inequality $|z|_p \geq B^{-C_4}$ is also valid if $|z|_p = 1$. Since z is an S–unit, the product formula yields

$$|z| = \prod_{p \in S} |z|_p^{-1} \leq B^{sC_4}.$$

Hence

$$2^B \leq B^{sC_4},$$

which produces an upper bound for B,

$$\frac{B}{\log B} \leq \frac{sC_4}{\log 2},$$

hence an upper bound for M.

□

Similar results hold for the S–unit equation where the unknown are S–units in an algebraic number field. They play a crucial role in Diophantine Geometry.

5.4 An explicit lower bound

We give only one example of an explicit estimate which can be proved by means of transcendental number theory. Here is the main result from [LN1819].

Theorem 5.6 (Yu. V. Nesterenko)**.** *Let $a_1, \dots, a_n$ be positive rational numbers such that the real values of logarithms $\log a_1, \dots, \log a_n$ are linearly independent over $\mathbb{Q}$. Then for any set of integers $b_1, \dots, b_n$ with $B = \max |b_j| > 0$, the following inequality holds:*

$$|b_1 \log a_1 + \cdots + b_n \log a_n| \geq \exp\{-2.9(2\mathrm{e})^{2n+6}(n+2)^{9/2}\mathrm{h}(a_1)\cdots\mathrm{h}(a_n)\log(\mathrm{e}B)\}.$$

5.5 Conjectures

The second part of Lang's book [ECDA] deals with measures of linear independence for logarithms of algebraic numbers (not only for the usual exponential function, but also for elliptic functions). The introduction to Chap. X and XI of [ECDA, pp.212–217] proposes far reaching conjectures. For instance:

Conjecture 5.7. *For any $\epsilon > 0$, there exists a constant $C_5(\epsilon) > 0$ such that, for any nonzero rational integers $a_1, \dots, a_n$, $b_1, \dots, b_n$ with $a_1^{b_1} \cdots a_n^{b_n} \neq 1$*

$$\left| a_1^{b_1} \cdots a_n^{b_n} - 1 \right| \geq \frac{C_5(\epsilon)^n}{B^{n-1+\epsilon} A^{n+\epsilon}},$$

where $A = \max_{1 \leq i \leq n} |a_i|$ and $B = \max_{1 \leq i \leq n} |b_i|$.

See also [GL326, § 1.2] for further comments including the *abc*–Conjecture.

References

[ECDA] S. Lang, *Elliptic curves: Diophantine analysis.* Grund. der Math. Wiss. **231**, Springer-Verlag (1978).

[LN1819] Yu. V. Nesterenko. *Linear forms in logarithms of rational numbers*. Diophantine approximation (Cetraro, 2000), 53–106, Lecture Notes in Math., **1819**, Springer, Berlin (2003).

References to courses on transcendental numbers

• Samit Dasgupta. *Introduction to Transcendence Theory.* Duke University, 2021.
https://services.math.duke.edu/~dasgupta/Transcendence/index.html

• Adam J Harper. *A version of Baker's theorem on linear forms in logarithms* (1st December 2010).
https://warwick.ac.uk/fac/sci/maths/people/staff/harper/bakernotes.pdf

• Kannan Soundararajan. *Transcendental Number Theory.* Math 249A Fall 2010. A course by LATEXed by Ian Petrow, September 19, 2011
http://math.stanford.edu/~ksound/TransNotes.pdf