Berhampur, IISER, Decembre 2018. updated: 07812/2018

Introduction to Diophantine Approximation

Michel Waldschmidt[1]
http://www.math.jussieu.fr/∼miw/

1 First course: December 6, 2018.

Real numbers, rationals, irrationals. We denote by $\mathbb{Z}$ the ring of rational integers, by $\mathbb{Q}$ the field of rational numbers, by $\mathbb{R}$ the field of real numbers and by $\mathbb{C}$ the field of complex numbers. Given a real number, we want to know whether it is rational or not, that means whether it belongs to $\mathbb{Q}$ or not. The set of irrational numbers $\mathbb{R} \setminus \mathbb{Q}$ has no nice algebraic properties: it is not stable by addition nor by multiplication.
How to prove that a number is irrational?
Decimal, binary expansion. A real number is rational if and only if its decimal (or in any base $g \geq 2$) expansion is ultimately periodic.
Exercise: given $a/b \in \mathbb{Q}$, write $b = 2^{k_1}5^{k_2}b_1$ with $k_1 \geq 0$, $k_2 \geq 0$, $\gcd(b_1, 10) = 1$. Set $k = \max\{k_1, k_2\}$. Check that there exists $h \geq 1$ such that $10^h \equiv 1 \pmod{b_1}$. Write $10^h - 1 = \ell b_1$ and

$$\frac{a}{b} = \frac{2^{k-k_1}5^{k-k_2}\ell a}{10^k(10^h - 1)}.$$

Decimal expansion of $\sqrt{2}$, of e. Borel conjecture; normal numbers.
Continued fraction: of $\sqrt{2}$, of e, of π.

Rational approximation
Density of $\mathbb{Q}$ in $\mathbb{R}$.

The main tool in Diophantine approximation is the basic property that *any non-zero integer has absolute value at least* 1. There are many corollaries of this fact. The first one we consider here is the following:
If ϑ is a rational number, there is a positive constant $c = c(\vartheta)$ such that, for any rational number p/q with $p/q \neq \vartheta$,

$$\left|\vartheta - \frac{p}{q}\right| \geq \frac{c}{q}. \tag{1.1}$$

This result is obvious: if $\vartheta = a/b$ then an admissible value for c is $1/b$, because the non-zero integer $aq - bp$ has absolute value at least 1.

This property is characteristic of rational numbers: a rational number cannot be well approximated by other rational numbers, while an irrational number can be well approximated by rational numbers.

We now give several such a criterion.

[1]Faculté de Mathématiques Pierre et Marie Curie, Université Paris VI

Lemma 1.2 (Irrationality criterion)**.** *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*

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

(iii) *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*

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

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

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

According to this implication, in order to prove that some number is irrational, it is sufficient (and in fact also necessary) to produce good rational approximations. Lemma 1.2 tells us that an irrational real number ϑ has very good *friends* among the rational numbers, the sharp inequality (iv) shows indeed that ϑ is well approximated by rational numbers. Conversely, the proof we just gave shows that a rational number has *no good friend*, apart from himself. Hence in this world of rational approximation it suffices to have one good friend (not counting oneself) to guarantee that one has many very good friends.

Proof of Dirichlet's Theorem (i)⇒(iii) . The implications (iii)⇒(iv)⇒(ii)⇒(i) in Lemma 1.2 are easy. It only remains to prove (i)⇒(iii), which is a Theorem due to Dirichlet. For this we shall use the *box* or *pigeon hole* principle.

Let $Q > 1$ be given. Define $N = \lceil Q \rceil$: this means that N is the integer such that $N - 1 < Q \leq N$. Since $Q > 1$, we have $N \geq 2$.

For $x \in \mathbb{R}$ write $x = \lfloor x \rfloor + \{x\}$ with $\lfloor x \rfloor \in \mathbb{Z}$ (integral part of x) and $0 \leq \{x\} < 1$ (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

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

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

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

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 $1 \leq q \leq N - 1$ 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. This exercise extends the irrationality criterion Lemma 1.2 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

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

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

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

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

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

2 Second course: December 7, 2018.

Schanuel's Conjecture. *Let $x_1, \ldots, x_n$ be $\mathbb{Q}$–linearly independent complex numbers. Then among the $2n$ numbers $x_1, \ldots, x_n, e^{x_1}, \ldots, e^{x_n}$, there exists a subset $\{y_1, \ldots, y_n\}$ of n numbers which are algebraically independent: for any non–zero polynomial $P \in \mathbb{Q}[T_1, \ldots, T_n]$, the number $P(y_1, \ldots, y_n)$ is not 0.*
Assume Schanuel's Conjecture. Deduce that the number $\log \pi$ is transcendental. More generally, for any nonzero algebraic number, the two numbers e^α and π are algebraically independent. As a consequence, the number π cannot be written as the tangent, the cosine, the sine,... of an algebraic number.
`N.B. Such results are not known unconditionally.`

The following result improves the implication (i)⇒(iv) of Lemma 1.2.

Lemma 2.1. *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*

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

Of course the implication (ii)⇒(i) in Lemma 2.1 is weaker than the implication (iv)⇒(i) in Lemma 1.2. What is new is the converse.

Classical proofs of the equivalence between (i) and (ii) in Lemma 2.1 involve either continued fractions or Farey series.

Denote by $\Phi = 1.6180339887499\ldots$ the Golden ratio, which is the root > 1 of the polynomial $X^2 - X - 1$. The discriminant of this polynomial is 5. Recall also the definition of the Fibonacci sequence $(F_n)_{n \geq 0}$:

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

Lemma 2.2. *For any $q \geq 1$ and any $p \in \mathbb{Z}$,*

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

On the other hand

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

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

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

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

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

Hence

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

The first part of Lemma 2.2 follows.

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

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

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

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

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

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

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

By induction one easily checks

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

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

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

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

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

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

Hence

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

This proof of Lemma 2.2 can be extended by replacing $X^2 - X - 1$ by any irreducible polynomial with integer coefficients (see below Lemma 2.5).

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 2.1 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 2.1 the number $\sqrt{5}$ by a larger number.

If one omits these irrational numbers in the field generated by the Golden ratio, then Hurwitz showed that one can replace $\sqrt{5}$ by $2\sqrt{2}$, and again this is optimal. This is the beginning of the so-called *Markoff* [2] *spectrum* $\sqrt{5}$, $\sqrt{8}$, $\sqrt{221}/5$, $\sqrt{1517}/13$, ... which tends to $1/3$ and is obtained as follows. First consider the set of integers m for which the *Markoff equation*

$$m^2 + m_1^2 + m_2^2 = 3mm_1m_2$$

has a solution in positive integers (m_1, m_2) with $0 < m_1 \leq m_2 \leq m$. The infinite increasing sequence of these integers m starts with

$$1,\ 2,\ 5,\ 13,\ 29,\ 34,\ 89,\ 169,\ 194,\ 233,\ 433,\ 610,\ 985,\ 1325,\ 1597, \ldots \quad (2.3)$$

and there is an easy and well known algorithm to construct it: apart from $(1, 1, 1)$ and $(2, 1, 1)$, for any solution (m, m_1, m_2) there are three exactly solutions sharing two components with (m, m_1, m_2), namely

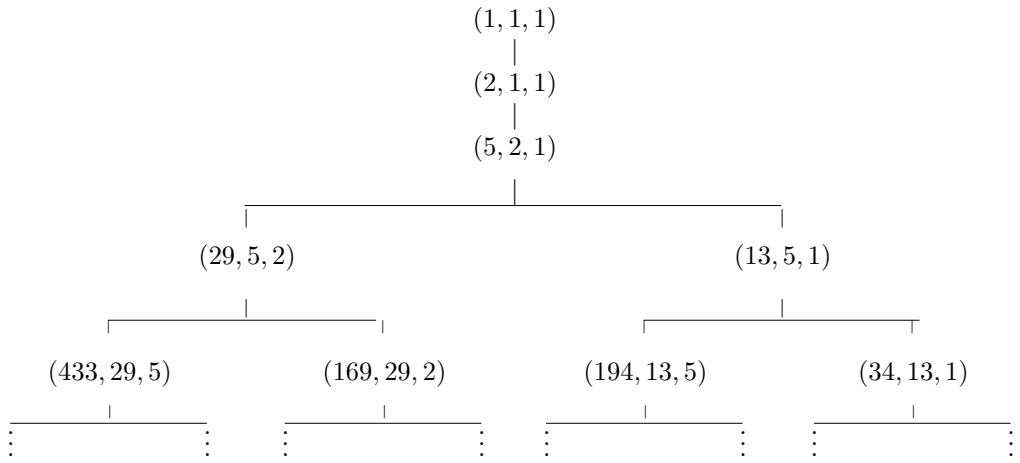
$$(m', m_1, m_2), \quad (m, m_1', m_2), \quad (m, m_1, m_2'),$$

where

$$m' = 3m_1m_2 - m, \quad m_1' = 3mm_2 - m_1, \quad m_2' = 3mm_1 - m_2.$$

[2] His name is spelled *Markov* in probability theory.

This produces the *Markoff tree*



For each m in the Markoff sequence (2.3), we define

$$\mu_m = \frac{\sqrt{9m^2 - 4}}{m}.$$

Then there is an explicit quadratic form $f_m(x, y)$ such that $f_m(x, 1) = 0$ and there is a root α_m of f_m for which

$$\liminf_{q \in \mathbb{Z},\ q \to \infty} (q \|q\alpha_m\|) = \frac{1}{\mu_m},$$

where $\|\cdot\|$ denotes the distance too the nearest integer:

$$\|x\| = \min_{m \in \mathbb{Z}} |x - m| = \min\big\{\{x\}\,;\, 1 - \{x\}\big\}.$$

The sequence of $(m, f_m, \alpha_m, \mu_m)$ starts as follows,

m	1	2	5	13
$f_m(x, 1)$	$x^2 + x - 1$	$x^2 + 2x - 1$	$5x^2 + 11x - 5$	$13x^2 + 29x - 13$
α_m	$[0; \overline{1}]$	$[0; \overline{2}]$	$[0; \overline{2211}]$	$[0; \overline{221111}]$
μ_m	$\sqrt{5}$	$\sqrt{8}$	$\sqrt{221}/5$	$\sqrt{1517}/13$

The third row gives the continued fraction expansion for α_m.

Exercise 2. Check that any solution (m, m_1, m_2) of Markoff's equation (2.3) is in Markoff's tree.

Irrationality of e

That e is not quadratic follows from the fact that the continued fraction expansion of e, which was known by L. Euler in 1737 is not periodic:

$$e = 2 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{4 + \cfrac{1}{\ddots}}}}}} = [2,\ 1,\ 2,\ 1,\ 1,\ 4,\ 1,\ 1,\ 6,\ 1,\ 1,\ 8, \dots]$$

Since this expansion is infinite we deduce that e is irrational. The fact that it is not ultimately periodic implies also that e is not a quadratic irrationality, as shown by Lagrange in 1770 – Euler knew already in 1737 that a number with an ultimately periodic continued fraction expansion is quadratic.

An easy and well known proof of the irrationality of e was given by J. Fourier in his course at the École Polytechnique in 1815. The main idea was to truncate the exponential series giving the value of e at some point N, which produces good enough approximations of e to use the irrationality criterion. Here is a simplification, found by Liouville, who proves the irrationality of e^{-1} instead of e, and avoids estimating the remainder.

We truncate the exponential series giving the value of e^{-1} at some point N:

$$N!\ e^{-1} - \sum_{n=0}^{N} \frac{(-1)^n N!}{n!} = \sum_{k \geq 1} \frac{N!(-1)^{N+k}}{(N+k)!}\cdot \tag{2.4}$$

The right hand side of (2.4) is a sum of an alternating series with general term tending to 0, its absolute value is bounded by the absolute value of the first term, which is positive and < 1. Hence the left hand side of (2.4) cannot be an integer. It follows that for any integer $N \geq 1$ the number $N!e$ is not an integer, which means that e is an irrational number.

Recall that the ring $\mathbb{Z}[X]$ is factorial, its irreducible elements of positive degree are the non-constant polynomials with integer coefficients which are irreducible in $\mathbb{Q}[X]$ (i.e. not a product of two non-constant polynomials in $\mathbb{Q}[X]$) and have content 1. The *content* of a polynomial in $\mathbb{Z}[X]$ is the greatest common divisor of its coefficients.

The *minimal polynomial* of an algebraic number α is the unique irreducible polynomial $P \in \mathbb{Z}[X]$ which vanishes at α and has a positive leading coefficient.

The next lemma is a variant of Liouville's inequality that we shall study more throughly later.

Lemma 2.5. *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 $q\alpha$. In particular

$$\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{2}.$$

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

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

and

$$q^d P(p/q) = a_0 q^d \prod_{i=1}^{d} \left(\frac{p}{q} - \alpha_i\right). \tag{2.6}$$

Also

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

The left hand side of (2.6) is a rational integer. It is not zero because P is irreducible of degree ≥ 2. For $i \geq 2$ we use the estimate

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

We deduce

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

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

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

□

The next corollary of Lemma 2.5 was proved by J. Liouville in 1844: this his how he constructed the first examples of transcendental numbers. His first explicit examples were given by continued fractions, next he gave further examples with series like

$$\theta_a = \sum_{n \geq 0} a^{-n!} \tag{2.7}$$

for any integer $a \geq 2$.

Lemma 2.8. *For any algebraic number α, there exist two constants c and d such that, for any rational number $p/q \neq \alpha$,*

$$\left|\alpha - \frac{p}{q}\right| \geq \frac{c}{q^d}.$$

It follows also from Lemma 2.5 that in Lemma 2.8, one can take for d the degree of α (that is the degree of the minimal polynomial of α).

Exercise 3. Denote by $P \in \mathbb{Z}[X]$ the minimal polynomial of α.
(a) Prove this result with d the degree of P and κ given by

$$\kappa = \max\big\{1\ ;\ \max_{|t-\alpha|\le 1} |P'(t)|\big\}.$$

(b) Check also that the same estimate is true with again d the degree of P and κ given by

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

where a_0 is the leading coefficient and $\alpha_1, \dots, \alpha_d$ 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.

3 Third course: December 8, 2018.

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

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

It follows from Lemma 2.8 that Liouville numbers are transcendental. In dynamical systems one says that 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 us check that the numbers (2.7) are Liouville numbers: let $a \ge 2$ be an integer and $\kappa > 0$ a real number. For sufficiently large N, set

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

Then we have

$$0 < \theta_a - \frac{p}{q} = \sum_{k\ge 1} \frac{1}{a^{(N+k)!-N!}}\cdot$$

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

$$(N+k)! - N! \ge N!N(N+1)\cdot(N+k-1) \ge N!\big(N + (k-1)!\big),$$

which yields

$$0 < \theta_a - \frac{p}{q} \leq \frac{e}{q^N}.$$

Diophantine approximation and Diophantine Equations In 1909 A. Thue found a connection between Diophantine equation and refinements of Liouville's estimate. We restrict here on one specific example.

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 2.5 with $P(X) = X^3 - 2$, $c = 3\sqrt[3]{4} < 5$). Thue was the first to achieve an improvement of the exponent 3. A explicit estimate was then obtained by A. Baker

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

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

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

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* $q > 0$,

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

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

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

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

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

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

Write

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

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

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

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

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

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

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

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

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

using (ii), we deduce

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

and (i) easily follows.

□

Diophantine Approximation: historical survey

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

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

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

From Dirichlet's box principle (see (i)⇒(iv) in Lemma 1.2) it follows that any irrationality exponent κ satisfies $\kappa \geq 2$. 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*.

From Liouville's inequality in Lemma 2.8 it follows that any irrational algebraic real number α has a finite irrationality exponent $\leq d$. Liouville numbers are by definition exactly the irrational real numbers which have no finite irrationality exponent.

For any $\kappa \geq 2$, there are irrational real numbers ϑ for which κ is an irrationality exponent and is the best: no positive number less than κ is an irrationality exponent for ϑ. Examples due to Y. Bugeaud in connexion with the triadic Cantor set 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 $d \geq 3$. Then any $\kappa > (d/2) + 1$ is an irrationality exponent for α.*

The fact that the irrationality exponent is $< d$ has very important corollaries in the theory of Diophantine equations. We gave an example above with $\sqrt[3]{2}$; here is the more general result of Thue on 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 $p/q \in \mathbb{Q}$,

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

(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

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

is an irrationality exponent for α. With $j=[\sqrt{d}]$ it follows that $2\sqrt{d}$ is an irrationality exponent for α. Dyson and Gel'fond in 1947 independently refined Siegel's estimate and replaced the hypothesis in Thue's Theorem 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.*

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

References:

• Diophantine approximation and Diophantine equations.
https://webusers.imj-prg.fr/~michel.waldschmidt/articles/pdf/HRI2011.pdf

• Introduction to Diophantine methods: irrationality and transcendence
https://webusers.imj-prg.fr/~michel.waldschmidt/articles/pdf/IntroductionDiophantineMethods.pdf