1. Approximation to real numbers by rationals

Objekttyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **17 (1971)**

Heft 1: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **21.07.2024**

0. Introduction

Our subject is part of the more general field of *diophantine approximation,* i.e. the study of rational approximation to real numbers. Books on diophantine approximation in general are due to Minkowski (1907) [1]), Koksma (1936), Cassels (1957), Niven (1963) and Lang (1966b), and a p-adic version is treated by Lutz (1955).

In the present survey we shall be concerned with the more special problem of rational approximation to real *algebraic* numbers. Contributions to this problem were first made by Liouville (1844), and deep theorems were proved among others by Thue (1908), Siegel (1921a), Roth (1955a) and Baker (1968b). We shall also discuss the more general questions of approximation to an algebraic number by algebraic numbers in a fixed number field or by algebraic numbers of fixed degree, and the question of simultaneous approximation to real algebraic numbers by rationals. As is well known, many results on approximation to algebraic numbers have applications to diophantine equations.

Of the books listed above, the one by Cassels (1957) has a chapter (ch. VI) on approximation to algebraic numbers. This subject also is the main topic in the book by Mahler (1961) and is the topic of chapter 6 of Le Veque (1955), of Kapitel 1 of Schneider (1957) and of chapter 6 of Lang (1962). Also see Lang (1971) and chapter 1 of Feldman and Shidlovskii (1967).

Until recently all the deep theorems on approximation to algebraic numbers were obtained by the method of Thue, Siegel and Roth, and accordingly most of the present survey is devoted to this method. In view of Baker's (1968b) results it is possible that the method of Gelfond and Baker will play an increasing role in the future. Rather than attempting to give a complete account of the literature, I tried to explain the main ideas in the proofs of the principal theorems.

1. Approximation to real numbers by rationals

1.1. This section is intended for the benefit of a reader who is not familiar with diophantine approximation, to provide a background for the

[1]) References are listed at the end. They are listed alphabetically by the name of the author, by the year, and finally by *a*, *b*, ... if there are several works by the same author in the same year.

more special problem of approximation to real algebraic numbers which will be discussed later.

THEOREM 1A (Dirichlet 1842). *Suppose* α *is a real number and* Q *is a real number greater than* 1. *Then there are integers* p, q *with*

$$1 \leqq q < Q \quad and \quad |\alpha q - p| \leqq Q^{-1}. \tag{1.1}$$

Let us recall the well known proof. Every real number ξ may be written as

$$\xi = [\xi] + \{\xi\},$$

where $[\xi]$ is a rational integer, the *integer part* of ξ, and where $\{\xi\}$, the *fractional part* of ξ, satisfies $0 \leqq \{\xi\} < 1$. Assume now that Q is an integer. The $Q + 1$ numbers

$$0, 1, \{\alpha\}, \{2\alpha\}, \ldots, \{(Q-1)\alpha\}$$

lie in the unit-interval $0 \leqq \xi \leqq 1$; hence there are two of these numbers whose difference has absolute value at most Q^{-1}. Thus there are integers r_1, r_2, s_1, s_2 with $0 \leqq r_i \leqq Q - 1$ $(i=1, 2)$ and $r_1 \neq r_2$ such that

$$|(r_1\alpha - s_1) - (r_2\alpha - s_2)| \leqq Q^{-1}.$$

If, say, $r_1 > r_2$, then $p = s_1 - s_2$ and $q = r_1 - r_2$ satisfy (1.1). This proves Dirichlet's Theorem when Q is an integer.

Now suppose that Q is *not* an integer. Since $Q' = [Q] + 1$ is an integer, there are integers p, q with $1 \leqq q < Q'$ and $|\alpha q - p| \leqq Q'^{-1}$, whence with $1 \leqq q < Q$ and $|\alpha q - p| < Q^{-1}$.

1.2. The greatest common factor of integers p, q will be denoted by (p, q). It is clear that in Dirichlet's Theorem one could stipulate that $(p, q) = 1$. The inequalities (1.1) in Dirichlet's Theorem yield

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}. \tag{1.2}$$

COROLLARY 1B. *Suppose that* α *is irrational. Then there exist infinitely many rationals* p/q *with* $(p, q) = 1$ *and with* (1.2).

For since α is irrational, the inequality $|\alpha q - p| \leqq Q^{-1}$ in (1.1) can for fixed integers p, q with $q \neq 0$ hold only for bounded values of Q, say for $Q \leqq Q_0(p, q)$. Hence as $Q \to \infty$, there will be infinitely many distinct pairs of coprime integers p, q in Dirichlet's Theorem, giving rise to infinitely many rationals p/q with (1.2).

One should remark that this corollary does not hold for rationals α. For if $\alpha = a/b$ and if $p/q \neq a/b$, then

$$\left| \alpha - \frac{p}{q} \right| \geqq | bq |^{-1} > \frac{1}{q^2} \text{ if } | q | > | b | .$$

Corollary 1B can be strengthened:

THEOREM 1C (Hurwitz 1891).

(i) *For every irrational* α *there are infinitely many rationals* p/q *with* $(p, q) = 1$ *and with*

$$\left| \alpha - \frac{p}{q} \right| < \frac{1}{\sqrt{5}\, q^2} . \tag{1.3}$$

(ii) *This would no longer be true if* $\sqrt{5}$ *were replaced by a larger constant.*

The second statement can easily be proved: Suppose α is a real quadratic irrational and suppose there are infinitely many rationals p/q with

$$\left| \alpha - \frac{p}{q} \right| < \frac{1}{Aq^2} . \tag{1.4}$$

Let $P(x) = ax^2 + bx + c$ be a polynomial with rational integer coefficients and with root α; then $P(x) = a(x-\alpha)(x-\alpha')$ where α' is the conjugate of α. For every p/q with (1.4) we have

$$\frac{1}{q^2} \leqq \left| P\left(\frac{p}{q}\right) \right| = \left| \alpha - \frac{p}{q} \right| \left| a\left(\alpha' - \frac{p}{q}\right) \right| < \frac{1}{Aq^2} \left| a\left(\alpha' - \alpha + \alpha - \frac{p}{q}\right) \right|$$
$$< \frac{\sqrt{D}}{Aq^2} + \frac{| a |}{A^2 q^4} ,$$

where $D = b^2 - 4ac = a^2 (\alpha - \alpha')^2$ is the discriminant of P. It follows that $A \leqq \sqrt{D}$. In the special case when $\alpha = \dfrac{\sqrt{5} - 1}{2}$, $P(x) = x^2 + x - 1$, we have $D = 5$ whence $A \leqq \sqrt{5}$.

Note that $\dfrac{1}{\sqrt{5}}$ is a quadratic irrationality. It can be shown that the numbers α for which this constant is best possible are certain numbers in the quadratic number field generated by $\sqrt{5}$.

One calls an irrational number α *badly approximable* if there is a $c = c(\alpha) > 0$ such that

$$\left| \alpha - \frac{p}{q} \right| > \frac{c(\alpha)}{q^2}$$

for every rational p/q. We have just seen that the quadratic irrationals are badly approximable.

1.3. Certain results on diophantine approximation are closely related to continued fractions. Continued fractions are discussed in the books mentioned at the beginning, and a fuller account of them is given in Perron (1954). The rational function

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{\cdot}{\cdot \cdot + \cfrac{1}{a_n}}}}$$

will be denoted by $[a_0, a_1, \ldots, a_n]$ and will be called a *continued fraction.* Every rational number r may be written $r = [a_0, a_1, \ldots, a_n]$ where $n \geqq 0$ and where a_0 is an integer and $a_1, \ldots, a_n$ are positive integers. For every irrational α there exist unique rational integers $a_0, a_1, a_2, \ldots$ such that $a_1, a_2, \ldots$ are positive and $\lim_{n\to\infty} [a_0, a_1, \ldots, a_n] = \alpha$. The integers $a_0, a_1, a_2, \ldots$ are called the *partial quotients* of the *continued fraction expansion* of α. Define coprime integers p_n, q_n with $q_n > 0$ by $p_n/q_n = [a_0, a_1, \ldots, a_n]$. The rationals p_n/q_n converge to α, and they are called the *convergents to* α. These convergents are important for diophantine approximation because it can easily be shown that

$$\frac{1}{(a_{n+1}+2)\, q_n^2} < \left| \alpha - \frac{p_n}{q_n} \right| < \frac{1}{a_{n+1} q_n^2} \tag{1.5}$$

for every $n \geqq 0$, which implies in particular that $\left| \alpha - \frac{p_n}{q_n} \right| < \frac{1}{q_n^2}$, and because it was shown by Legendre that if

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

then $\frac{p}{q}$ is necessarily a convergent to α. It follows that α is badly approximable precisely if the partial quotients of the continued fraction expansion of α are bounded. In particular, the real quadratic irrationals have bounded partial quotients. (In fact it is well known that these numbers have a " periodic " continued fraction expansion.)

1.4. We have seen that for certain irrationals α the number $\frac{1}{\sqrt{5}}$ in (1.3) cannot be replaced by a smaller factor. But for most irrationals α the inequality (1.3) can be improved:

THEOREM 1D (Khintchine 1926b). *Suppose $\psi(q)$ is a positive, non-increasing function defined for $q = 1, 2, \ldots$. Consider the inequality*

$$\left| \alpha - \frac{p}{q} \right| < \frac{\psi(q)}{q} \tag{1.6}$$

and the sum

$$\sum_{q=1}^{\infty} \psi(q) . \tag{1.7}$$

If the sum is convergent, then (1.6) *has only finitely many solutions in rationals p/q with $q > 0$ for almost all α (in the sense of Lebesgue measure). If the sum is divergent, then* (1.6) *has infinitely many solutions for almost all α.*

In particular, for every $\delta > 0$, the inequality

$$\left| \alpha - \frac{p}{q} \right| < \frac{1}{q^{2+\delta}} \tag{1.8}$$

has only finitely many solutions for almost all α, but

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2 \log q} \tag{1.9}$$

has infinitely many solutions for almost all α.

Given a number like $\sqrt{2}$, e, π or $\sqrt[3]{2}$, it is of interest to know whether it behaves like almost every number. Quadratic irrationals are badly approximable and hence behave like almost every number with respect to (1.8) but not with respect to (1.9). From the known continued fraction expansion of e it is easy to deduce that neither of the inequalities (1.8), (1.9) has infinitely many solutions if $\alpha = e$. Mahler (1953) showed that $\left|\pi - \frac{p}{q}\right| < q^{-42}$ has only finitely many solutions, and Wirsing (unpublished) could reduce 42 to 21. The behavior of $\sqrt[3]{2}$ and of real algebraic numbers in general will be discussed in the next section.

2. Approximation to algebraic numbers by rationals. Roth's Theorem

2.1. Theorem 2A (Liouville 1844). *Suppose α is a real algebraic number of degree d. Then there is a constant $c(\alpha)$* [1] *> 0 such that*

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

for every rational $\frac{p}{q}$ distinct from α.

This theorem was used by Liouville to construct transcendental numbers. For example, put $\alpha = \sum_{v=1}^{\infty} 2^{-v!}$, $q(k) = 2^{k!}$, $p(k) = 2^{k!} \sum_{v=1}^{k} 2^{-v!}$. Then

$$\left|\alpha - \frac{p(k)}{q(k)}\right| = \sum_{v=k+1}^{\infty} 2^{-v!} < 2 \cdot 2^{-(k+1)!} = 2\left(q(k)\right)^{-k-1}.$$

Hence for any d and any constant $c > 0$ one has

$$\left|\alpha - \frac{p(k)}{q(k)}\right| < \frac{c}{\left(q(k)\right)^d}$$

---

[1]) The constants $c, c_1, c_2, \ldots$ of different subsections are independent.