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

Objekttyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

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

Heft 1: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **24.09.2024**

Nutzungsbedingungen

Die ETH-Bibliothek ist Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Inhalten der Zeitschriften. Die Rechte liegen in der Regel bei den Herausgebern.
Die auf der Plattform e-periodica veröffentlichten Dokumente stehen für nicht-kommerzielle Zwecke in Lehre und Forschung sowie für die private Nutzung frei zur Verfügung. Einzelne Dateien oder Ausdrucke aus diesem Angebot können zusammen mit diesen Nutzungsbedingungen und den korrekten Herkunftsbezeichnungen weitergegeben werden.
Das Veröffentlichen von Bildern in Print- und Online-Publikationen ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Die systematische Speicherung von Teilen des elektronischen Angebots auf anderen Servern bedarf ebenfalls des schriftlichen Einverständnisses der Rechteinhaber.

Haftungsausschluss

Alle Angaben erfolgen ohne Gewähr für Vollständigkeit oder Richtigkeit. Es wird keine Haftung übernommen für Schäden durch die Verwendung von Informationen aus diesem Online-Angebot oder durch das Fehlen von Informationen. Dies gilt auch für Inhalte Dritter, die über dieses Angebot zugänglich sind.

Ein Dienst der *ETH-Bibliothek*
ETH Zürich, Rämistrasse 101, 8092 Zürich, Schweiz, www.library.ethz.ch

http://www.e-periodica.ch

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

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 q^{-42}$ has only finitely many solutions, and Wirsing (unpublished) could reduce 42 to 21.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.

if k is large. By Liouville's Theorem, α cannot be algebraic of any degree d, and hence α is transcendental.

For the sake of later refinements we shall break the extremely simple proof of Liouville's Theorem into three parts (a), (b) and (c).

(a) Let $P(x)$ be the *defining polynomial* of α, i.e. the polynomial of degree d with root α which has coprime integer coefficients and a positive leading coefficient.

(b) Taylor's formula yields

$$\left| P\left(\frac{p}{q}\right) \right| = \left| \sum_{i=1}^{d} \left(\frac{p}{q} - \alpha\right)^i \frac{1}{i!} P^{(i)}(\alpha) \right| < \frac{1}{c(\alpha)} \left| \frac{p}{q} - \alpha \right|$$

if

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

(c) $P\left(\frac{p}{q}\right) \neq 0$, whence $\left| P\left(\frac{p}{q}\right) \right| \geqq \frac{1}{q^d}$, and combining this with (b) we obtain Liouville's Theorem if $\left| \frac{p}{q} - \alpha \right| \leqq 1$. The Theorem is obvious if $\left| \frac{p}{q} - \alpha \right| > 1$.

2.2. Now suppose that α is a real algebraic number of degree d and consider the inequality

$$\left| \alpha - \frac{p}{q} \right| < \frac{1}{q^\mu}, \tag{2.1}$$

where $\frac{p}{q}$ is rational with a positive denominator q. By Liouville's Theorem this inequality has only finitely many solutions if $\mu > d$. Thue (1908, 1909) made the important discovery that this is still true under the weaker assumption that $\mu > (d/2) + 1$. Then Siegel (1921a) showed that it suffices to have $\mu > 2\sqrt{d}$. (Actually his result was slightly better, with a more complicated function in place of $2\sqrt{d}$.) These results of Thue and of Siegel will be referred to as Thue's Theorem and as Siegel's Theorem. Dyson (1947) improved $\mu > 2\sqrt{d}$ to $\mu > \sqrt{2d}$. (See also Gelfond (1952), ch. 1.) Finally

Roth (1955a) showed that (2.1) with $\mu > 2$ has only finitely many solutions. His result may be formulated as follows.

THEOREM 2B. *Suppose α is a real algebraic number. Then for every $\delta > 0$ there are only finitely many distinct rationals $\frac{p}{q}$ with $q > 0$ and with*

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^{2+\delta}}. \tag{2.2}$$

In view of Dirichlet's Theorem, the exponent 2 is best possible here. But it is conceivable that the factor q^{δ} could be replaced by a smaller factor. But nothing is known in this direction. The metrical result (Theorem 1D) suggests that

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2 (\log q)^{1+\delta}}$$

has only finitely many solutions for every positive δ. The first written account of this conjecture appears to be in Lang (1965a).

For real quadratic irrationals α we have $\left|\alpha - \frac{p}{q}\right| > \frac{c(\alpha)}{q^2}$ by Liouville's Theorem (or by the fact that α is badly approximable, as was shown below Theorem 1C). Hence for such numbers α, Liouville's Theorem is stronger than Roth's Theorem. It is not known whether there exists an algebraic number of degree $d \geqq 3$ whose partial quotients are bounded, or whether there exists such a number whose partial quotients are unbounded. In view of Theorem 1D it is likely that every algebraic number of degree $d \geqq 3$ has unbounded partial quotients. Some numerical evidence for this was given by von Neumann and Tuckerman (1955), Richtmyer et al. (1962), and Bruyno (1964).

2.3. Let us see how much Roth's Theorem tells us about the partial quotients. In view of (1.5) it shows that

$$a_{n+1} < q_n^{\delta}$$

for every $\delta > 0$ and for $n > n_0(\alpha, \delta)$. Now it is well known that $q_0 = 1$, $q_1 = a_1 q_0 + 1$ and that $q_n = a_n q_{n-1} + q_{n-2}$ for $n \geqq 2$, hence that $q_n \leqq (a_1 + 1) \ldots (a_n + 1)$, and we obtain

(2.3) $$a_{n+1} < ((a_1+1)\dots(a_n+1))^{\delta}$$

for every $\delta > 0$ and for $n > n_1(\alpha, \delta)$. On the other hand one has

$$q_n > (a_n a_{n-1}+1)\, q_{n-2} \geqq ((a_n+1)(a_{n-1}+1))^{1/2}\, q_{n-2} > \dots$$
$$> ((a_n+1)\dots(a_1+1))^{1/2},$$

and this shows that the truth of (2.3) for every $\delta > 0$ and sufficiently large n is equivalent to Roth's Theorem. Davenport and Roth (1955) proved that for real algebraic irrationals α one has

$$\log\log q_n < \frac{c_1(\alpha)\, n}{\sqrt{\log n}}.$$

Further results on the continued fraction expansion of algebraic numbers were given by Baker (1962).

2.4. Cugiani (1959) could show that if $\frac{p(1)}{q(1)}, \frac{p(2)}{q(2)}, \dots$ are solutions of

$$\left|\alpha - \frac{p}{q}\right| < q^{-2-20\,(\log\log\log q)^{-1/2}}$$

with $0 < q(1) < q(2) < \dots$, then

(2.4) $$\limsup \frac{\log q(k+1)}{\log q(k)} = \infty.$$

Before Roth's Theorem was known, Schneider (1936) had shown that if $\frac{p(1)}{q(1)}, \frac{p(2)}{q(2)}, \dots$ with $0 < q(1) < q(2) < \dots$ are solutions of (2.2), then (2.4) holds. Schneider's Theorem in turn is a sharpening of a similar result of Siegel (1921b). Roth's Theorem enables one to prove the transcendency of a wider class of numbers than Liouville's Theorem, e.g. of $\alpha = \sum_{\nu=1}^{\infty} 2^{-3^{\nu}}$, but actually this can also be done with the earlier theorem of Schneider just mentioned.

2.5. Davenport and Roth (1955) have determined an explicit upper bound $B = B(\alpha, \delta)$ for the number of solutions of (2.2). However, at present one cannot give an upper bound $B^* = B^*(\alpha, \delta)$ for the denominators q of the solutions p/q of (2.2). Hence Roth's Theorem is " non-

effective ". It is easy to see that Liouville's Theorem is effective, but the theorems of Thue, Siegel and Dyson are also non-effective. Some further remarks on this question will be made in §3.6.

But effective bounds for weaker inequalities than (2.2) were given by Baker and will be discussed in §5.

2.6. Now suppose that $F(x, y)$ is a not identically vanishing binary form of degree $d \geqq 3$ with rational coefficients which has no multiple factors of positive degree. Such a binary form can be factored as

$$F(x, y) = L_1(x, y) \dots L_d(x, y)$$

where $L_i(x, y) = \gamma_i x + \delta_i y$ $(i = 1, \dots, d)$ are linear forms whose coefficients are real or complex algebraic numbers. Since F has no multiple factors, any two linear forms L_i, L_j with $i \neq j$ are linearly independent.

Let (x, y) be an integer point with $F(x, y) \neq 0$. By rearranging the factors $L_1, \dots, L_d$ we may assume that

$$0 < |L_1(x, y)| \leqq \dots \leqq |L_d(x, y)|.$$

Now if $\gamma_1 = 0$ or if δ_1/γ_1 is rational, then it is clear that $|L_1(x, y)| \geqq c_1$ with a positive c_1 independent of (x, y). If $\gamma_1 \neq 0$ and $y = 0$, then $|L_1(x, y)| = |\gamma_1| (|x| + |y|)$. Finally if $\gamma_1 \neq 0$, δ_1/γ_1 is irrational and $y \neq 0$, then $L_1(x, y) = \gamma_1 y \left(\frac{x}{y} - \alpha\right)$ with $\alpha = -\delta_1/\gamma_1$, and for every $\delta > 0$ one has $|L_1(x, y)| \geqq c_2(\delta) |y|^{1-2-\delta} \geqq c_2(\delta) (|x| + |y|)^{-1-\delta}$ by Roth's Theorem. (Roth's Theorem is trivially true if α is complex.) Therefore it is true in general that $|L_1(x, y)| \geqq c_3(\delta) (|x| + |y|)^{-1-\delta}$ with $c_3(\delta) > 0$. On the other hand since L_1, L_2 are linearly independent, we have

$$|L_d(x, y)| \geqq \dots \geqq |L_2(x, y)| \geqq \tfrac{1}{2} (|L_1(x, y)| + |L_2(x, y)|)$$
$$\geqq c_4 (|x| + |y|),$$

whence

$$|F(x, y)| \geqq c_3(\delta) c_4^{d-1} (|x| + |y|)^{-1-\delta+(d-1)} = c_5(\delta) (|x| + |y|)^{d-2-\delta}.$$

Thus the following holds.

THEOREM 2C. *Suppose $F(x, y)$ is a binary form of degree $d \geqq 3$ with rational coefficients and without multiple factors. Then for any $v < d - 2$ there are only finitely many integer points (x, y) with*

$$0 < |F(x, y)| < (|x| + |y|)^v.$$

COROLLARY 2D. *Suppose $F(x, y)$ is a binary form as in Theorem 2C and suppose $F(x, y)$ has no rational linear factor. Let $G(x, y)$ be a polynomial of total degree $v < d - 2$. Then there are only finitely many integer points (x, y) with*

$$F(x, y) = G(x, y). \tag{2.5}$$

Namely, such a form F has $0 < |F(x, y)|$ for any non-zero integer point (x, y). We deduced Theorem 2C and its corollary from Roth's Theorem. If instead we would have used Thue's or Siegel's Theorem, then we would have had to replace the condition $v < d - 2$ by the stronger condition $v < (d/2) - 1$ or $v < d - 2\sqrt{d}$, respectively. In particular, Thue's Theorem suffices to deal with the equation

$$F(x, y) = m \tag{2.6}$$

where m is a constant, which is often called " Thue's equation ".

Using his (1921a) result, Siegel (1929) could classify all algebraic curves defined over the rationals on which there are infinitely many integer points. In particular these curves must be of genus zero.

Schinzel (1968) used this result of Siegel to prove a theorem which implies that in Corollary 2D the assumption that $v < d - 2$ may be replaced by the weaker assumption that $v < d$. Roth's Theorem is not required to obtain this sharper version of Corollary 2D.

2.7. Mahler (1933b), (1933c) gave upper bounds for the number of solutions of Thue's equation (2.6). Davenport and Roth (1955) derived upper bounds for the number of solutions of the equation (2.5) of Corollary 2D. Siegel (1970) showed that there is an explicit such bound for Thue's equation (2.6) which depends only on m and the degree d if $F(x, y) = (\alpha x + \beta y)^d + (\gamma x + \delta y)^d$ with $\alpha\delta - \beta\gamma \neq 0$. (In particular, every form $F(x, y)$ of degree $d = 3$ may be written in this way.) Perhaps Siegel's conclusion is true for arbitrary forms $F(x, y)$.

Mahler (1933c) gave an asymptotic formula

$$N(m) \approx c_1(F)\, m^{2/d}$$

for the number $N(m)$ of solutions of $|F(x, y)| \leqq m$ in coprime integers x, y. Now let $N'(m)$ be the number of integers n with $|n| \leqq m$ which may be represented at least once as $n = F(x, y)$ with coprime x, y. Hooley (see (1967) and the references given there) developed powerful analytic methods to show that

$$N'(m) \approx c_2(F)\, m^{2/d}$$

if either $d = 3$ and the discriminant of F is not of some rather special type, or if $F(x, y) = x^d + y^d$ for some $d \geqq 3$. To generalize these results to arbitrary forms $F(x, y)$ appears to be extremely difficult.

The methods of Thue, Siegel and Roth do not enable one to find bounds for the size $|x| + |y|$ of solutions of Thue's equation, and hence they provide no method to find all the solutions of such an equation. Therefore these methods are called " non-effective ". Effective results will be discussed in §5.

3. An outline of the proof of Roth's Theorem

3.1. We shall follow Cassel's rearrangement (Cassels (1957), ch. VI) of Roth's proof. It is easy to see that we may restrict ourselves to the case when α is an algebraic *integer* of degree $d > 1$.

Suppose we tried to modify the proof of Liouville's Theorem as follows. In step (a) we pick a polynomial $P(x)$ with rational integer coefficients which has a root at α of order i and which has degree r. Next, in step (b) we suppose that

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^{\mu}}, \tag{3.1}$$

and Taylor's expansion

$$P\left(\frac{p}{q}\right) = \sum_{j=i}^{r} \left(\frac{p}{q} - \alpha\right)^j \frac{1}{j!} P^{(j)}(\alpha)$$

yields $\left|P\left(\frac{p}{q}\right)\right| \leqq cq^{-\mu i}$. Finally (c) we have $P\left(\frac{p}{q}\right) \neq 0$ whence $\left|P\left(\frac{p}{q}\right)\right| \geqq q^{-r}$ for all but finitely many rationals $\frac{p}{q}$. Hence if (3.1) has infinitely many solutions, then $\mu i \leqq r$ or

$$\mu \leqq \left(\frac{i}{r}\right)^{-1}.$$

Hence one should try to make $\frac{i}{r}$ as large as possible. But it is clear that