Lecture Notes in Mathematics

1819

D. Masser
Yu V. Nesterenko
H. P. Schlickewei
W. M. Schmidt
M. Waldschmidt

Diophantine Approximation

Cetraro, Italy 2000

Editors: F. Amoroso
U. Zannier

Springer

Fondazione
C.I.M.E.

D. Masser
H.P. Schlickewei
M. Waldschmidt
Yu. V. Nesterenko
W. M. Schmidt

Diophantine Approximation

Lectures given at the
C.I.M.E. Summer School
held in Cetraro, Italy,
June 28 – July 6, 2000

Editors: F. Amoroso
U. Zannier

Fondazione
C.I.M.E.

Springer

Authors and Editors

Francesco Amoroso
Laboratoire de Mathématiques
Nicolas Oresme, CNRS UMR 6139
Université de Caen, BP 5186
14032 Caen, France
e-mail: amoroso@math.unicaen.fr

Umberto Zannier
Instituto Universitario Architettura-D.C.A.
Santa Croce 191
300135 Venezia, Italy
e-mail: zannierqdimi.uniud.it

David Masser
Institute of Mathematics
Basel University
Rheinsprung 21
4051 Basel, Switzerland
e-mail: masser@math.unibas.ch

Yuri V. Nesterenko
Faculty of Mechanics
and Mathematics
Moscow State University
Vorob'evy Gory
119899 Moscow, Russia
e-mail: nest@trans.math.msu.su

Hans Peter Sclickewei
Department of Mathematics
Phillips University of Marburg
Hans-Meerwein-Str., Lahnberge
35032 Marburg, Germany
e-mail: hps@mathematik.uni-marburg.de

Wolfgang Schmidt
Department of Mathematics
University of Colorado
Boulder, CO 80309-0395, USA
e-mail: schmidt@euclid.colorado.edu

Michel Waldschmidt
Institut de Mathématiques
Université Paris VI
175 rue du Chevaleret
75013 Paris, France
e-mail: miw@math.jussieu.fr

Cataloging-in-Publication Data applied for

Bibliographic information published by Die Deutsche Bibliothek

Die Deutsche Bibliothek lists this publication in the Deutsche Nationalbibliografie; detailed bibliographic data is available in the Internet at http://dnb.ddb.de

Mathematics Subject Classification (2000): 11J68, 11J86, 11B37

ISSN 0075-8434
ISBN 3-540-40392-2 Springer-Verlag Berlin Heidelberg New York

Springer-Verlag Berlin Heidelberg New York a member of BertelsmannSpringer
Science + Business Media GmbH

http://www.springer.de

Printed in Germany

Typesetting: Camera-ready TEX output by the authors

SPIN: 10936825 41/3142/du - 543210 - Printed on acid-free paper

Preface

Diophantine Approximation is a branch of Number Theory having its origins in the problem of producing "best" rational approximations to given real numbers. Since the early work of Lagrange on Pell's equation and the pioneering work of Thue on the rational approximations to algebraic numbers of degree ≥ 3, it has been clear how, in addition to its own specific importance and interest, the theory can have fundamental applications to classical diophantine problems in Number Theory. During the whole 20th century, until very recent times, this fruitful interplay went much further, also involving Transcendental Number Theory and leading to the solution of several central conjectures on diophantine equations and class number, and to other important achievements. These developments naturally raised further intensive research, so at the moment the subject is a most lively one.

This motivated our proposal for a C.I.M.E. session, with the aim to make it available to a public wider than specialists an overview of the subject, with special emphasis on modern advances and techniques. Our project was kindly supported by the C.I.M.E. Committee and met with the interest of a large number of applicants; forty-two participants from several countries, both graduate students and senior mathematicians, intensively followed courses and seminars in a friendly and co-operative atmosphere.

The main part of the session was arranged in four six-hours courses by Professors D. Masser (Basel), H. P. Schlickewei (Marburg), W. M. Schmidt (Boulder) and M. Waldschmidt (Paris VI).

This volume contains expanded notes by the authors of the four courses, together with a paper by Professor Yu. V. Nesterenko (Moscow) – who was unable to accept our invitation to give an expected fifth course – concerning recent work by Matveev.

We shall now briefly illustrate the corresponding contents.

Masser's contribution concerns, roughly speaking, the modern theory of heights, starting with the most basic notions and then turning to the more sophisticated context of algebraic groups. This ample overview describes fundamental results and techniques in the subject, together with applications to transcendence problems. Masser also outlines the transcendence theory of elliptic logarithms and abelian functions (which he originally developed), and its important recent consequences toward outstanding diophantine problems on curves and abelian varieties.

Nesterenko's article is devoted to the proof of the nowadays best known lower bounds in Baker's theory of linear forms in logarithms of algebraic numbers. With the aim of stressing the new ideas introduced by Matveev, the

author concentrates on a situation slightly simpler in detail than the most general one, but containing all the important features of the methods.

Schlickewei deals with the celebrated Subspace Theorem. This result, originally discovered by W. M. Schmidt, is a far-reaching extension of Roth's Theorem on the approximations of an algebraic number by rationals, also covered in the lectures. Schlickewei describes the most recent sharpenings (such as the "absolute version"), obtained mainly in joint work by himself and J.-H. Evertse. Finally, he presents here his very recent work on a version of the theorem for approximation by algebraic numbers of bounded degree (obtained jointly with H. Locher).

Schmidt's article concerns the diophantine theory of linear recurrences, whose famous prototype is the Fibonacci sequence. He gives a general survey of the most important problems, methods and results, involving also S-unit equations and intersections of varieties with finitely generated multiplicative groups. In particular, he also illustrates the general strategy underlying his recent solution of an outstanding conjecture in the field; namely, *the zero-multiplicity of a non-degenerate linear recurrence is bounded only in terms of the "length" of the recurrence.*

Waldschmidt's contribution is on transcendence and linear independence over $\overline{\mathbb{Q}}$ of logarithms of algebraic numbers. Starting with Lindemann's classical theorems on the exponential function, he proceeds with the sophisticated results by A. Baker, which yield fundamental applications to effective diophantine analysis. Waldschmidt describes several approaches to the technically complicated proofs, clarifying the main ideas underlying methods which may confound the non-expert. He also details certain modern devices to obtain the best numerical bounds for the involved quantities.

The topics presented in such fine lecture notes incorporate many of the most fundamental methods and applications of Diophantine Approximation, giving an extremely broad viewpoint, precious for both beginners and experts. Also, the style of exposition has little in common with other contributions to the topic and the volume substantially enriches the existing literature.

It is a pleasure for us to thank the authors for their difficult work in coordinating the respective contributions, for their efforts in explaining the subtle points in the simplest and most effective style, and for working out these beautiful papers. We also thank the participants, whose enthusiasm was fundamental for the success of the session.

Finally, the editors express their thanks to Carlo Viola for his valuable advice and help concerning both the organization of the session and the preparation of the present volume.

Francesco Amoroso Umberto Zannier

C.I.M.E.'s activity is supported by:

Ministero dell'Università e della Ricerca Scientifica e Tecnologica, COFIN '99;

Ministero degli Affari Esteri – Direzione Generale per la Promozione e la Cooperazione – Ufficio V;

Consiglio Nazionale delle Ricerche;

E.U. under the Training and Mobility of Researchers Programme;

UNESCO-ROSTE, Venice Office.

Contents

Approximation of Algebraic Numbers

Linear Recurrence Sequences

Heights, Transcendence, and Linear Independence on Commutative Group Varieties

David Masser

Mathematisches Institut, Universität Basel

1 First lecture. Introduction and basic techniques

Of course it is impossible for four lecturers to cover the whole of diophantine approximation and transcendence theory in 24 hours. So each one has to restrict himself to special aspects.

These notes expand slightly on my original lectures, and I am grateful to Sinnou David for his comments on an earlier manuscript.

Let us start with perhaps the most basic problems, analogous to the Goldbach conjecture in analytic number theory. In 1744 Euler proved that the number e is irrational, and shortly after in 1761 Lambert did the same for π. We still don't know if $e + \pi$ is irrational, and no-one expects a proof soon.

Much later in 1873 Hermite proved that e is transcendental; that is, the only polynomial $P(X)$ with coefficients in the field $\mathbb{Q}$ of rational numbers satisfying $P(e) = 0$ is the zero polynomial. Shortly afterwards in 1882 Lindemann did the same for π. And a general 1934 result of Gelfond and Schneider implies the same for e^{π}.

It follows in particular that the value $\Gamma(1/2) = \sqrt{\pi}$ of the classical gamma function is also transcendental; for example if we have a non-trivial equation $P(\sqrt{\pi}) = 0$ then we can write $P(X) = XQ(X^2) - R(X^2)$ and it would follow that $\pi(Q(\pi))^2 = (R(\pi))^2$ giving a non-trivial equation for π. More generally, if $\mathbb{C}$ denotes the field of all complex numbers, the subset

$$\overline{\mathbb{Q}} = \{\alpha \text{ in } \mathbb{C} \text{ ; there is } P \neq 0 \text{ in } \mathbb{Q}[X] \text{ with } P(\alpha) = 0\}$$

is known to be a field. So $\sqrt{\pi}$ in $\overline{\mathbb{Q}}$ would imply π in $\overline{\mathbb{Q}}$, a contradiction.

We also know that $\Gamma(1/3)$ is transcendental, although this is a relatively recent result of 1976 or so obtained by Chudnovsky. The proof is however different in several respects: for $\Gamma(1/2)$, π and e one uses in an essential way the exponential function e^z, whereas for $\Gamma(1/3)$ one uses the Weierstrass elliptic

function $\wp(z)$ satisfying the differential equation $(\wp'(z))^2 = 4(\wp(z))^3 - 4$ (see Lecture 3). To this function is associated the elliptic curve E whose affine part is defined by $y^2 = 4x^3 - 4$; and so we have a commutative group variety or algebraic group. Actually we already had one with e^z; this function parametrizes the multiplicative group $\mathbb{G}_m$ whose complex points $\mathbb{G}_m(\mathbb{C})$ are the non-zero complex numbers $\mathbb{C}^*$.

In fact Chudnovsky uses also the function $\zeta(z)$ satisfying $\zeta'(z) = -\wp(z)$; this corresponds not to E but to a group extension G in the exact sequence

$$0 \to \mathbb{G}_a \to G \to E \to 0$$

with the additive group $\mathbb{G}_a$ (see Lecture 6). In fact we know rather more: the proof delivers the algebraic independence of $\Gamma(1/3)$ and π, which means that the only polynomial P in $\mathbb{Q}[X, Y]$ satisfying $P(\Gamma(1/3), \pi) = 0$ is $P = 0$. Taking P in $\mathbb{Q}[X]$ gives the transcendence of $\Gamma(1/3)$.

The topic of algebraic independence will however not be treated in these lectures. It was recently the subject of an instructional conference in Luminy; see Springer Lecture Notes 1752 "Introduction to algebraic independence theory".

Similarly by considering $y^2 = 4x^3 - 4x$ Chudnovsky proved the transcendence of $\Gamma(1/4)$.

More recently Nesterenko proved the algebraic independence of the three numbers π, e^π, $\Gamma(1/4)$, which was new even if $\Gamma(1/4)$ is omitted. The proof uses modular forms, for which there is no underlying group variety.

Going further, one hopes that in the next ten years the transcendence of $\Gamma(1/5)$, via the algebraic independence of π, $\Gamma(1/5)$ and $\Gamma(2/5)$, will be established using the curve $y^2 = 4x^5 - 4$. Right now we know only the algebraic independence of at least two of these numbers (see for example Chapter 3 of the recent Ph.D. Thesis of P. Grinspan). This curve has genus 2, and so we have to use the apparatus of Jacobians or more generally abelian varieties A or even extensions G satisfying

$$0 \to L \to G \to A \to 0$$

with $L = \mathbb{G}_a^r \times \mathbb{G}_m^s$ a linear group variety. And already such extensions include all commutative group varieties over $\overline{\mathbb{Q}}$.

It would be possible to start the present lecture course with a discussion of such general objects G; and possibly this suits the taste of several people in the audience. But I prefer to start with $\mathbb{G}_m$ and gradually work upwards; thus the present Lecture 1 as well as Lecture 2 will stay on the $\mathbb{G}_m$ level. Then Lectures 3 and 4 will go elliptic, Lecture 5 abelian, and finally Lecture 6 will treat aspects of the general case. At present, as might be expected, we can do a lot more for simpler group varieties, and one would lose many subtleties by going rightaway to the general case.

Back to basics. Once we know that a number like π is transcendental it is natural to ask for more quantitative results; for example how small can $P(\pi)$

be for nonzero $P(X)$ in $\mathbb{Q}[X]$, or nearly equivalently how small can $|\pi - \alpha|$ be for α in $\overline{\mathbb{Q}}$? Thus Mahler in 1953 used Hermite's methods to prove

$$|\pi - r/s| > s^{-42} \tag{1.1}$$

for all rational integers r, s in $\mathbb{Z}$ with $s \geq 2$. This looks like a curiosity, but in fact in the case $G = \mathbb{G}_m^n$ (corresponding to Baker's Theorem – see the lectures of Michel Waldschmidt) these quantitative results are as important, if not more so, as the purely qualitative ones. Thus lower bounds for linear forms in logarithms can be applied to diophantine equations, class number problems, and so forth.

The elliptic analogues for E^n also have applications of a different sort to diophantine equations, and also to isogeny problems for elliptic curves (see Lecture 4). And those for A^n can be applied not only to isogenies but also to answer some interesting polarization questions for abelian varieties (see Lecture 5).

It will be unavoidable to talk about heights. These started life as a mere tool in the proofs, but they have gradually acquired a life of their own and are today the subject of intensive research. The original methods of transcendence theory are employed in order to prove results about heights which can then be applied in other areas of number theory. In particular the theory of lower bounds for heights is very active at the moment, and we will see examples in Lectures 2, 3 and 5.

Again back to basics. Before we begin with group varieties, let us give an example in Mahler's Method, where there is no natural underlying group variety, only a kind of "2-action". This method seems also to have provided some of the inspiration for the precursors of Nesterenko's Theorem mentioned above.

In general the technical nature of most of the material makes it impossible to give complete proofs. But as an exception we will now prove the irrationality of the number

$$\eta = 2/3 + (2/3)^2 + (2/3)^4 + (2/3)^8 + \cdots = \sum_{m=0}^{\infty} (2/3)^{2^m}.$$

Consider the "auxiliary polynomial"

$$P(X, Y) = 2XY^2 + 4XY - 3Y^2 + X - Y. \tag{1.AP}$$

This may well be the first explicit specimen that the reader has ever seen; however it will not be the last. Define the numbers

$$\alpha_n = P((2/3)^{2^{n+1}}, \eta_n) \qquad (n = 0, 1, 2, \ldots)$$

with

$$\eta_n = (2/3)^{2^{n+1}} + (2/3)^{2^{n+2}} + \cdots = \text{"tail" of } \eta.$$

Clearly α_n is rather small; certainly $O((2/3)^{2^{n+1}})$ as $n \to \infty$. But P was chosen to make it even smaller. One finds after a short calculation that

$$\alpha_n = -2(2/3)^{6.2^{n+1}} + \text{ higher powers of } (2/3)^{2^{n+1}}$$

and so

$$|\alpha_n| \le 3(2/3)^{6.2^{n+1}} < (1/10)^{2^{n+1}} \tag{1.UB}$$

if n is sufficiently large. Thus we gain an extra 6 in the exponent.

Now assume to the contrary that η is rational. It follows that

$$\alpha_n = P\left((2/3)^{2^{n+1}}, \eta - 2/3 - (2/3)^2 - \cdots - (2/3)^{2^n}\right)$$

is rational. We can estimate its denominator: if $\eta = r/s$ (r, s in $\mathbb{Z}$, $s \ge 1$) we find that $s_n = 3^{2^{n+1}}(s.3^{2^n})^2$ is one; that is, $s_n\alpha_n$ is in $\mathbb{Z}$. The "Fundamental Theorem of Transcendence" says that $|N| \ge 1$ if N is in $\mathbb{Z}$ with $N \ne 0$. It follows that

$$|\alpha_n| \ge 1/s_n = s^{-2}(1/9)^{2^{n+1}} \tag{1.LB}$$

provided

$$\alpha_n \ne 0. \tag{1.NV}$$

Now if n is large enough, (1.LB) contradicts (1.UB).

But why is $\alpha_n \ne 0$? This innocent question is here easy to answer, but it will become more and more of a nuisance until it almost takes over the subject. We will see the outcome in Lecture 6.

There are many ways of proving $\alpha_n \ne 0$. The fastest is analytic, and consists of checking that

$$\lim_{n\to\infty} \alpha_n/(2/3)^{6.2^{n+1}} = -2. \tag{1.2}$$

Thus $\alpha_n \ne 0$ for all n large enough. This is strong but the argument doesn't generalize too well, for example to several variables. An algebraic way is to observe that

$$\alpha_n = P(\xi_n, \eta_n), \qquad \xi_n = (2/3)^{2^{n+1}}.$$

Now the curve defined by $P = 0$ has infinitely many points, so there is no immediate contradiction from $\alpha_n = 0$. But

$$\alpha_{n+1} = Q(\xi_n, \eta_n), \qquad Q(X, Y) = P(X^2, Y - X).$$

The equations $P = Q = 0$ define an intersection of two curves and therefore probably a finite number of points. And indeed the resultant of P and Q (with respect to Y) is readily computed as

$$R(X) = 16X^{10} - 48X^9 + 36X^8 - 16X^7$$

(why are there so many zeros at $X = 0$?). Now if n is large enough then

$$\alpha_n \neq 0 \quad \text{or} \quad \alpha_{n+1} \neq 0$$

otherwise $R(\xi_n) = 0$, which is impossible. So (1.NV) holds for infinitely many n, and this weak assertion suffices for the above irrationality proof.

In some ways this proof is typical. The steps can be designated as follows (their order is not too important, and it is sometimes logically better to interchange the last two):

- (AP) - construction of auxiliary polynomial,
- (UB) - obtaining an upper bound,
- (LB) - obtaining a lower bound,
- (NV) - proving the non-vanishing.

One can replace 2/3 in the preceding example by any other rational ζ with $0 < |\zeta| < 1$, although the step (AP) can no longer be done explicitly, making the other steps correspondingly more difficult.

What lies behind (1.AP)? Of course $\eta = f(2/3)$ for the analytic function

$$f(z) = \sum_{m=0}^{\infty} z^{2^m}.$$

Now P is chosen such that the function

$$\varphi(z) = P(z, f(z))$$

has a zero of order 6 at $z = 0$; its Taylor expansion there starts with $-2z^6$. Further $\alpha_n = \varphi\big((2/3)^{2^{n+1}}\big)$ and so we see (1.2) more clearly.

For an explanation with interpolation determinants see Waldschmidt's lectures (section 2.1).

If we replace 2/3 with say 1999/2000 then $P(X, Y)$ has to have degree at most 22796 in each variable, with φ having a zero of order at least 519703208, and its coefficients are rational integers of size probably about $10^{10^{13}}$. So there is no hope of seeing the polynomial explicitly.

In general if P has degree at most L in each variable, then φ can have a zero of order at least $T = (L+1)^2 - 1$; and the proofs work because L^2 grows faster than L. Of course the functional equation $f(z^2) = f(z) - z$ also plays a crucial role.

We should also note the following. Even though we cannot write $P(X, Y)$ down, it must of course be non-zero. The algebraic independence over $\mathbb{Q}$ (and even over $\mathbb{C}$) of the functions z and $f(z)$ is easy to verify, and therefore $\varphi(z) = P(z, f(z))$ is not identically zero. So the above analytic proof of (1.NV) generalizes immediately.

A more serious difficulty is the step from irrationality to transcendence. It was Mahler in 1929 who proved that $f(\zeta)$ is transcendental whenever ζ is algebraic with $0 < |\zeta| < 1$. He used an *ad hoc* version of (LB); in particular it no longer suffices to consider the denominator alone. See the book [56] of Nishioka for a complete proof (pp. 1-5), as well as an excellent general account.

A substitute for the denominator can easily be found. Any α in $\overline{\mathbb{Q}}$ satisfies an equation $P(\alpha) = 0$ with $P(X)$ in $\mathbb{Q}[X]$, and one can assume that

(i) $P(X)$ is irreducible over $\mathbb{Q}$,
(ii) $P(X) = a_0 X^d + \cdots + a_d$ with coprime $a_0, \ldots, a_d$ in $\mathbb{Z}$ and $a_0 > 0$.

Then $P(X)$ is unique, and its degree d is the degree $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ of α; and if $d = 1$ this a_0 is the denominator of α. Unfortunately any inequality $|\alpha| \geq 1/F(a_0)$ is no longer true if $d > 1$, so we need more than just a_0. Formerly one took $\max\{|a_0|, \ldots, |a_d|\}$, but one gets much better functorial properties first by factorizing $P(X)$ over $\mathbb{C}$ (or $\overline{\mathbb{Q}}$) as

$$P(X) = a_0 \prod_{i=1}^{d} (X - \alpha_i)$$

for the conjugates $\alpha_1, \ldots, \alpha_d$; and then by defining

$$H(\alpha) = \left(a_0 \prod_{i=1}^{d} \max\{1, |\alpha_i|\} \right)^{1/d}. \tag{1.3}$$

The exponent $1/d$ is needed for properties such as

$$H(\alpha^m) = (H(\alpha))^{|m|}$$

for all m in $\mathbb{Z}$, which is not quite trivial to prove even for $m = 2$ (see Lecture 2).

Examples are $H(1999/2000) = 2000$, $H(26/65) = 65$ and more generally

$$H(r/s) = \max\{|r|, s\}$$

for coprime r, s in $\mathbb{Z}$ with $s \geq 1$. Or $H(\sqrt{2}) = \sqrt{2}$ and more generally $H(2^{1/d}) = 2^{1/d}$ for every $d \geq 1$ in $\mathbb{Z}$. And $H(1 - \sqrt{2}) = \sqrt{1 + \sqrt{2}}$, $H(\sqrt{-6}) = \sqrt{6}$, $H(1 + \sqrt{-6}) = \sqrt{7}$, $H(1 + \sqrt[3]{2}) = \sqrt[3]{3}$. Or $H(e^{\pi i/5}) = 1$ and more generally $H(\tau) = 1$ for every root of unity τ. And finally

$$H(1 - e^{\pi i/5}) = \sqrt{\frac{1}{2}(1 + \sqrt{5})} = H\left(\frac{1}{2}(1 + \sqrt{5})\right)$$

and, selected at random,

$$H(1/(\rho^2 - 5\rho + 50)) = \sqrt[3]{147200}$$

for $\rho^3 - 7\rho + 10 = 0$.

Now (LB) takes the form

$$|\alpha| \geq (H(\alpha))^{-d} \tag{1.4}$$

for any $\alpha \neq 0$ in $\overline{\mathbb{Q}}$. For the proof one notes that $H(\alpha^{-1}) = H(\alpha)$ is easy, and then

$$(H(\alpha^{-1}))^d \geq \max\{1, |\alpha^{-1}|\} \geq |\alpha|^{-1}.$$

As soon as one is accustomed to this height function, one may go ahead and prove the general result on $f(\zeta)$ referred to above. For example, to show that $f(2/3)$ is not an algebraic number of degree at most 1999 one uses an auxiliary polynomial $P(X, Y)$ of degree at most $L = 8119$ in each variable, with the parameter n tending to infinity. But to establish the transcendence of $f(2/3)$ this degree L must also be allowed to go to infinity, independently of n.

The algebraic independence over $\mathbb{Q}$ of z and $f(z)$ is now necessary not only for the proof, but also for the truth of Mahler's result. A vivid illustration of this was accidentally provided by Mahler himself. In [43] he used the functions z and

$$g(z) = \sum_{m=0}^{\infty} z^{2^m}/(1 - z^{2^{m+1}})$$

apparently to prove the transcendence of $\eta = g(\frac{1}{2}(1 - \sqrt{5}))$. In terms of the Fibonacci numbers $f_0 = 1$, $f_1 = 1$, $f_2 = 2, \ldots$ of Wolfgang Schmidt's lectures (section 1), we find that

$$\sum_{n=0}^{\infty} 1/f_{2^n} = 2 - \eta$$

and is therefore also transcendental. After publication it was however pointed out that the sum is $\frac{1}{2}(7 - \sqrt{5})$! The explanation is that z and $g(z)$ are not algebraically independent and indeed $g(z) = z/(1 - z)$.

A similar phenomenon occurred in my thesis [44] (Chapter 3) when I was attempting to prove the linear independence of five numbers connected with an elliptic function in the case of complex multiplication. I failed; apart from incompetence the only imaginable explanation was the algebraic dependence of certain functions, and it turned out that this dependence did lead back to an unexpected (at least by me) linear relation between three of the five numbers.

Very recently Corvaja and Zannier have given another approach to the transcendence of numbers like $f(\zeta) = \sum_{m=0}^{\infty} \zeta^{2^m}$ which does not use functional equations. It is based on the Subspace Theorem with several valuations, and in view of the accompanying lectures of Hans Peter Schlickewei it seems appropriate to sketch the ideas, for simplicity in the context of irrationality.

We then require the p-adic valuations $|\ \ |_p$ on $\mathbb{Q}$ defined for each positive prime p by $|p|_p = 1/p$ and $|q|_p = 1$ for every integer q not divisible by p, together with multiplicativity $|xy|_p = |x|_p|y|_p$ and $|0|_p = 0$. We already have $|x|_\infty = |x|$ the standard archimedean valuation.

For example to prove the irrationality of $\eta = f(2/3)$ above, one could note that $\eta = r/s$ would differ from the rational number $\eta - \eta_n$ by the small quantity η_n. This by itself does not lead to a contradiction, even if we take into account the special denominator of $\eta - \eta_n$ by working also 3-adically. Instead

one subtracts off an extra $(2/3)^{2^{n+1}}$ from η_n to get $\eta_{n+1} = O((2/3)^{2^{n+2}})$ which is even smaller, and one works 2-adically as well. In terms of the linear forms

$$\begin{aligned} M_\infty(X,Y) &= X+Y, & N_\infty(X,Y) &= Y, \\ M_2(X,Y) &= X+Y, & N_2(X,Y) &= Y, \\ M_3(X,Y) &= X, & N_3(X,Y) &= Y, \end{aligned}$$

evaluated at $(x_n, y_n) = (3^{2^n} r_n, -2^{2^{n+1}} s)$ with $r_n = 3^{2^n} s\,\eta_n$ in $\mathbb{Z}$ one finds

$$\begin{aligned} |M_\infty(x_n,y_n)|_\infty &= 3^{2^{n+1}} s\,\eta_{n+1}, & |N_\infty(x_n,y_n)|_\infty &= 2^{2^{n+1}} s, \\ |M_2(x_n,y_n)|_2 &\le 1, & |N_2(x_n,y_n)|_2 &\le 2^{-2^{n+1}}, \\ |M_3(x_n,y_n)|_3 &\le 3^{-2^n}, & |N_3(x_n,y_n)|_3 &\le 1, \end{aligned}$$

and that as $n \to \infty$ the product is $O(\theta^{2^n})$ with $\theta = 16/27$. Now the rational Subspace Theorem with $S = \{\infty, 2, 3\}$ (see Schlickewei's lectures, section 1 or his original papers [65], [66] especially Theorem 4.1 p. 395, [67] or also [70] Theorem 1D p. 177) easily supplies the required contradiction; all we need is $\theta < 1$ (and earlier results like Ridout's would have sufficed).

If we again replace 2/3 by $\zeta = 1999/2000$ then it is now the S-units $\zeta^{2^{n+1}}, \ldots, \zeta^{2^{n+13}}$ that should be subtracted off from the "almost S-unit" $f(\zeta) - \zeta - \cdots - \zeta^{2^n}$ with $S = \{\infty, 2, 5, 1999\}$, and the Subspace Theorem in 14 variables can be used. However an extra argument is needed to eliminate the exceptional subspaces of dimension 13.

See [18] for several other applications of these ideas.

One down, five to go...

2 Second lecture. More on heights

In the last lecture we saw how to define a height function H from the set $\overline{\mathbb{Q}}$ of all algebraic numbers to the real interval $[1, \infty)$, principally as a measuring device. But it has remarkable functorial properties, making it useful for a variety of problems, and many of these problems lead to the same fundamental question: how small can its values be?

We already noted in Lecture 1 that $H(\tau) = 1$ for all roots of unity τ. Kronecker's Theorem of 1857 says that $H(\alpha) > 1$ for all other $\alpha \neq 0$. But $H(2^{1/d}) = 2^{1/d}$ for all positive integers d, so $H(\alpha)$ can get arbitrarily close to 1. On the other hand $(H(2^{1/d}))^d = 2$ is bounded away from 1, and in 1933 Lehmer [42] asked if $(H(\alpha))^d$ is generally bounded away from 1 for all algebraic numbers $\alpha \neq 0$ of degree d that are not roots of unity. In fact Lehmer restricted himself to algebraic integers, because otherwise $a_0 \ge 2$ in (1.3) of Lecture 1 and so already $(H(\alpha))^d \ge 2$. The answer is still unknown, and Lehmer himself found the smallest value so far, which is $(H(\alpha_{10}))^{10} = 1.176\ldots$, with $P(\alpha_{10}) = 0$ for