Lecture Notes in Mathematics 1559

Vladimir G. Sprindžuk

# Classical Diophantine Equations

$$F(x_0, y) = F_1(y) \cdots F_r(y)$$

$$\sum_{\theta_p \in F_j} \frac{\ln a_p}{\ln |a|} = \frac{d_j}{n} + O\left(\sqrt{\frac{\ln H_F}{\ln |a|}}\right) \qquad (1 \leq j \leq r)$$

Springer-Verlag

Vladimir G. Sprindžuk

# Classical Diophantine Equations

Springer-Verlag
Berlin Heidelberg New York
London Paris Tokyo
Hong Kong Barcelona
Budapest

Author

Vladimir G. Sprindžuk †

Translation Editors

Ross Talent †

Alf van der Poorten
Centre for Number Theory Research
Macquarie University
NSW 2109, Australia

Title of the original Russian edition: Klassicheskie diofantovy uravneniya ot dvukh neizvestnykh. "Nauka". Moscow 1982.

Mathematics Subject Classification (1991): 11J86, 11D00, 11J68, 12E25

ISBN 3-540-57359-3 Springer-Verlag Berlin Heidelberg New York
ISBN 0-387-57359-3 Springer-Verlag New York Berlin Heidelberg

Library of Congress Cataloging-in-Publication Data. Sprindzhuk, V. G. (Vladimir Gennadievich) [Klassicheskie diofantovy uravneniia ot dvukh neizvestnykh. English] Classical diophantine equations / Vladimir G. Sprindzhuk. p. cm. – (Lecture notes in mathematics; 1559) Includes bibliographical references and index.
ISBN 3-540-57359-3 (Berlin: acid-free) – ISBN 0-387-57359-3 (New York: acid-free) 1. Diophantine equations. I. Title. II. Series: Lecture notes in mathematics (Springer-Verlag); 1559. QA3.L28 no. 1559 [QA242] 512'.74–dc20 93-33443

2146/3140-543210 - Printed on acid-free paper

# Editorial Policy

§ 1. Lecture Notes aim to report new developments - quickly, informally, and at a high level. The texts should be reasonably self-contained and rounded off. Thus they may, and often will, present not only results of the author but also related work by other people. Furthermore, the manuscripts should provide sufficient motivation, examples and applications. This clearly distinguishes Lecture Notes manuscripts from journal articles which normally are very concise. Articles intended for a journal but too long to be accepted by most journals, usually do not have this "lecture notes" character. For similar reasons it is unusual for Ph. D. theses to be accepted for the Lecture Notes series.

§ 2. Manuscripts or plans for Lecture Notes volumes should be submitted (preferably in duplicate) either to one of the series editors or to Springer- Verlag, Heidelberg . These proposals are then refereed. A final decision concerning publication can only be made on the basis of the complete manuscript, but a preliminary decision can often be based on partial information: a fairly detailed outline describing the planned contents of each chapter, and an indication of the estimated length, a bibliography, and one or two sample chapters - or a first draft of the manuscript. The editors will try to make the preliminary decision as definite as they can on the basis of the available information.

§ 3. Final manuscripts should preferably be in English. They should contain at least 100 pages of scientific text and should include

- a table of contents;
- an informative introduction, perhaps with some historical remarks: it should be accessible to a reader not particularly familiar with the topic treated;
- a subject index: as a rule this is genuinely helpful for the reader.

Further remarks and relevant addresses at the back of this book.

# Lecture Notes in Mathematics 1559

Subseries:
LOMI and Euler International
Mathematical Institute, St. Petersburg

# Foreword

The author had initiated a revision and translation of this volume prior to his death.

Given the rapid advances in transcendence theory and diophantine approximation over recent years, one might fear that the present monograph, which is essentially a translation of a work originally published in the then USSR in 1982, is mostly superseded. That is not so. There is in any event a certain amount of updating inserted by the author. However, the author's emphasis remains original and almost unique, and well warrants study now that this work appears in the mathematical *lingua franca** thus making it easily accessible to the majority of mathematicians.

Most research mathematicians will be familiar with the eccentricities of Russian style — in this case I should correct that to Byelorussian style — in mathematical writing. There is quite an amount of repetitive detail and little assumption about notation, exemplified by a great deal more 'letting' in enunciations of lemmata and theorems than now seems customary; and the natural logarithm remains ln, just as on the engineer's calculator. Notwithstanding that, Sprindžuk maintains a pleasant and chatty approach, full of wise and interesting remarks. His emphases well warrant emulation.

I had the pleasure of meeting the author at several Oberwolfach meetings. Indeed, it was his instruction 'You will walk with me,' that led to the one and only time that I have allowed myself to be subjected to the post-breakfast perambulation all the way down and then, worse, back up the drive. I was a little surprised to find that Sprindžuk's spoken English was rather better than I had been led to expect given his apparent reticence at tea and dinner. But that may have been a function of the bad old days.

Nonetheless, the translation from which the present volume is derived was just from Russian to 'Russlish'. I am indebted, in the first instance to the late Ross Talent who commenced TEXing and 'translating' the translation prior to his death in a car accident in September 1991, and then to Sam Williams and Dr Deryn Griffiths who assisted with preliminary typing of the remainder of the manuscript. I owe special and extensive thanks to Dr Chris Pinner who carefully read all that preliminary typescript and carefully annotated it with corrections both to its TEX and to its mathematics. Incidentally, Chris Pinner's efforts make it clear that at least some of the detail provided must be

* I cannot resist using this phrase and irritating my French colleagues.

taken flexibly. What is presented here is entirely correct in spirit; that is, in its principal parameters. In applying it one should, as always, rework the details to the purpose at hand. That will be all the more so given the errors I will inadvertently have introduced, notwithstanding all the efforts of my minders.

I have gone to some pains to translate from the Russlish to English, but restrainedly, if only so as not to hide Sprindžuk's style and personality. That may mean the retention of some eccentric phrasing. I hope that I have not done so to such an extent as to hide important meaning. However, once or twice, I should confess, I had no idea what was intended, even after retreating to the original Russian. So it goes.

I began by saying that much of this monograph remains fresh, interesting and useful. The reader should notice the unusual emphases in the first seven chapters; I am confident that there is much yet to be usefully done along the lines there delineated. I am not aware of any other place that a reader can find a congenial entry to the ideas of the final two chapters and am certain that the present volume will spark a great deal of useful thought and fascinating work.

Alfred J. van der Poorten
ceNTRe for Number Theory Research
Macquarie University
alf@mpce.mq.edu.au

Sydney, Australia
May 1993

Afterword: In mid-1993, a volume on diophantine equations seems incomplete if it fails to allude to the surprising announcement by Andrew Wiles of his proof of the Shimura-Taniyama-Weil conjecture for semi-stable elliptic curves, and its spectacular consequence. As it happens, Fermat's Last Theorem gets barely a mention in the present volume; the one oasis is the concluding remarks of Chapter VII. Thus to bring this volume up to date in this respect it suffices just to eliminate mention of a paper of Inkeri and mine! Of course it is no longer totally out of the question that the work on elliptic curves be extended to prove the *abc* conjecture; that will warrant a rather more significant revision.

July 1993

# Preface

The theory of diophantine equations has a long history, and like human culture as a whole, has had its ups and downs. This monograph aims to show that the last 10 to 15 years were a period of uplift, at least in the field of diophantine equations in two integral unknowns, a part of the subject which has intrigued and attracted researchers throughout its history.

Even a cursory acquaintance with the work preceding the papers of Runge [166] in 1887 and Thue [229] in 1909 will impress with the dramatic search for general laws for the behaviour of solutions of diophantine equations, and the realisation of the peculiar difficulties of attaining this aim (see, for example, [56], vol. 2). It was Runge who obtained the first general theorem on the finiteness of the number of integer points on a wide variety of algebraic curves. After nearly a century it is difficult to judge the influence of Runge's work on his contemporaries. Certainly it is evident in Hilbert's proof of his irreducibility theorem [98], which initiated research on the inverse problem of Galois theory. It is possible that Thue was stimulated by Runge's arguments to investigate the representation of numbers by irreducible binary forms, a closely related problem not covered by Runge's theorem. However, the peculiar virtue of Runge's methods – the possibility of making them effective and obtaining explicit bounds for the solutions – was lost in both cases.

Thue's work initiated a most fruitful period of development of the theory of diophantine equations in two unknowns – the golden age of ineffective methods! Two monumental results of that period are widely known: Siegel [193] proved that curves of genus greater than zero have only finitely many integer points, and Roth [165], in the problem of representation of numbers by irreducible binary forms (the Thue equation), obtained the best possible exponent estimate for the unknowns in terms of the number represented. Both results were achieved by a thorough development and enrichment of Thue's method, and on the way to these results many specific facts were obtained, special methods were worked out, and phenomena arising from these two general theorems were discovered. The monographs by Skolem [196], Lang [120], Mahler [136] and Mordell [145] give a good idea of the variety of the results obtained.

One of the above-mentioned special methods is among the most beautiful in the theory of diophantine equations: Skolem's method. Though Skolem himself and his adherents achieved much by this method, and were for a long time the leaders in questions of number representation by norm forms in three or more variables, the ascendancy was finally won by Thue's method (Schmidt's theory of representation of numbers by norm forms is a fine testament to that [185]). Nevertheless, the fundamental idea of Skolem's method, the reduction of algebraic diophantine equations to exponential equations, has shown exceptional vitality in recent episodes of the theory of diophantine equations.

In 1952 Gelfond [77] suggested that non-trivial effective estimates for linear forms in the logarithms of three or more algebraic numbers would make it possible to obtain explicit bounds for the solutions of exponential diophantine equations, in particular those to which Thue's equation reduces, thereby yielding an effective bound for the solutions of this equation. By that time the necessary estimates were known in the case of two logarithms, but the transition to three logarithms presented considerable difficulty and had not been carried through. In 1966 Baker [8] obtained such estimates for forms in logarithms of any number of algebraic numbers, and later applied them to diophantine equations. Baker's work had a stimulating effect on his close colleagues, and during the next decade the theory of diophantine equations was enriched by results of a qualitatively new type, which will occupy a considerable portion of this monograph.

This book covers all the main types of diophantine equations in two unknowns for which the solutions are to be integers or $S$-integers or rationals or algebraic numbers from a fixed field. Such a broad notion of solution domain makes available a wider arsenal of arithmetic facts than would be possible if only the classical case of rational integer solutions (which, of course, remains the main case here as well) were considered. In particular, by transcending the rational integer domain, we are able to analyse certain classes of diophantine equations in several unknowns (for example, representations of numbers by certain norm forms). Special attention is given to the influence of the parameters of the equation on the magnitude of its solutions, and to the construction (in principle) of best possible bounds for the solutions. Here an interesting general phenomenon is observed which formerly revealed itself in very special cases only: the regulator of some algebraic number field connected with the equation has a preeminent influence on the magnitude of the equation's solutions. (In virtue of the Siegel-Brauer formula, this amounts to preeminence of the class number.) We use this phenomenon to describe parametric construction of algebraic number fields with large class number. Further work in this direction may lead to major improvements to known bounds for solutions of diophantine equations in terms of the height of the equation, or to a proof that such an improvement is impossible (which seems more probable). Not all results concerning the value of class numbers are directly connected with the theory of linear forms in logarithms of algebraic numbers, but they were inspired by the above-mentioned relationship between class numbers and the value of solutions of diophantine equations. Chapter IX is altogether independent of the theory of logarithms.

The theory of algebraic units, the theory of ideals in algebraic number fields, and the concepts and techniques of $p$-adic analysis in both arithmetic and analytic form predominate in this monograph. The informed reader will notice that $p$-adic analysis makes some quite unexpected appearences. Many of the results can be obtained without the use of $p$-adic analysis, but there are some which cannot even be formulated without reference to $p$-adic metrics (See Chap. IX).

There is also another approach to the investigation of integer points on algebraic curves which uses parametrisation of curves and the Mordell-Weil theorem on the group of rational points on the curve. We do not touch upon this approach, because the main results obtained in this way are still ineffective. Besides, this topic is treated in a recent monograph by Lang [124].

I have often seen the admiration felt for modern diophantine analysis by older mathematicians who have worked in number theory or taken an interest in its development; for what is done now was in their youth just a pleasant dream. Younger mathematicians will take its achievements for granted, and will feel that its deficiencies should be criticised. If this monograph should stimulate them to creative work or offer clues to new discoveries, its aims will be more than fulfilled.

As this work was nearing completion, it became clear that for many readers it will make an impression much as the one tourists in Paris feel on seeing the Pompidou Centre: all the main lines, informative and logical, are extremely plain and to the fore. It is, of course, easier to construct a building or write a book in the 'good old style', but then inevitably a great deal will be hidden for the sake of a favourable external impression. Extreme frankness, whether in art or science, imposes much more on our time.

Central themes of this monograph were the subject of my lectures at the Institut Henri Poincaré (Paris, May-June 1980) by invitation of the Université de Paris VI. Namely, (1) generalisations and effective improvements to Liouville's inequality, (2) a connection between bounds for the solutions of diophantine equations and class numbers, and also the manner in which the class number varies, (3) effective versions of Hilbert's irreducibility theorem and rational points on algebraic curves. The audience's interest in and attention to these topics helped to finalise their presentation in this monograph. Michel Waldschmidt and Daniel Bertrand contributed most of all. I am obliged to Alan Baker for the exceptional stimulus which his works gave me in the late sixties, and to Andrzej Schinzel for information given to me during previous investigations of Hilbert's theorem. I am heartily grateful to all the above-mentioned persons.

Minsk
September 1980

V. Sprindžuk

# Notation

The following notation, mainly standard, is frequently used.

| | |
|---|---|
| $\mathbb{Q}$ | the field of rational numbers |
| $\mathbb{C}$ | the field of complex numbers |
| $\overline{\mathbb{Q}}$ | the field of all algebraic numbers |
| $\mathbb{K}, \mathbb{L}, \ldots$ | algebraic number fields of finite degree over $\mathbb{Q}$ |
| $[\mathbb{L} : \mathbb{Q}]$ | the degree of the field $\mathbb{L}$ |
| $[\mathbb{L} : \mathbb{K}]$ | the degree of $\mathbb{L}$ over $\mathbb{K}$ |
| $\mathbb{Z}$ | the ring of rational integers |
| $I_{\mathbb{K}}$ | the ring of integers of $\mathbb{K}$ |
| $\mathbb{K}(x, y, \ldots)$ | the field of rational functions in $x, y, \ldots$ over $\mathbb{K}$ |
| $\mathbb{K}[x, y, \ldots]$ | the ring of polynomials in $x, y, \ldots$ over $\mathbb{K}$ |
| $E_{\mathbb{K}}$ | the group of units of the field $\mathbb{K}$ |
| $D_{\mathbb{K}}$ | the discriminant of $\mathbb{K}$ |
| $R_{\mathbb{K}}$ | the regulator of $\mathbb{K}$ |
| $h_{\mathbb{K}}$ | the number of ideal classes of $\mathbb{K}$ |
| $\mathrm{N}(\mathfrak{a})$ | the absolute norm of an ideal $\mathfrak{a}$ |
| $\mathrm{Nm}(\alpha)$ | the absolute norm of an algebraic number $\alpha$ |
| $\mathrm{Nm}_{\mathbb{L}/\mathbb{K}}(\alpha)$ | the absolute norm from $\mathbb{L}$ to $\mathbb{K}$ of an algebraic number $\alpha$ |
| $h(\alpha)$ | the height of an algebraic number $\alpha$ |
| $\lceil\alpha\rceil$ | the size of an algebraic number (the maximum modulus of the conjugates of $\alpha$) |
| $\deg \alpha$ | the degree of an algebraic number $\alpha$ |
| $\mathrm{ord}_{\mathfrak{p}}\, \alpha$ | the exponent of the power to which a prime ideal $\mathfrak{p}$ divides $\alpha$ |
| $\vert\ \vert_p$ | the $p$-adic metric, normalised so that $\vert p\vert_p = p^{-1}$ |
| $\mathbb{Q}_p$ | the field of $p$-adic numbers |
| $\mathbb{Z}_p$ | the ring of $p$-adic integers |
| $\overline{\mathbb{Q}}_p$ | the algebraic closure of $\mathbb{Q}_p$ |
| $\Omega_p$ | the completion in $\vert\ \vert_p$ of an algebraic closure of $\mathbb{Q}_p$ |
| $\lceil F\rceil$ or $H_F$ | the height of a polynomial $F$ |
| $\deg F$ | the degree of a polynomial $F$ |
| $\deg_x F$ | the degree of a polynomial $F$ with respect to $x$ |
| $D(F)$ | the discriminant of a polynomial $F$ |
| $R(F, G)$ | the resultant of polynomials $F$ and $G$ |
| $R_x(F, G)$ | the resultant of polynomials $F$ and $G$ with respect to $x$ |
| $c(n), c(n, \epsilon) \ldots$ | positive quantities depending only on the indicated parameters |
| $\ln x$ | the 'natural logarithm' of $x$, the logarithm to base $e$ |
| $\lfloor a \rfloor$ | the integer part of a real number $a$. |

# Table of Contents

# I. Origins

*This chapter reviews the origin and development of the fundamental principles of the contemporary analysis of diophantine equations, from the perspective of the theory of diophantine approximation.*

## 1. Runge's Theorem

Let $F(x,y)$ be an integral polynomial irreducible in $\mathbb{Q}[x,y]$. We suppose as we may without loss of generality that its degree in $y$ is at least its degree in $x$ and set $\deg_y F(x,y) = n \geq 2$. We consider solutions in integers $x$, $y$ of the equation

$$F(x,y) = 0. \tag{1.1}$$

Although Fermat and Euler had analysed special equations of this form (for example, $x^2 - Dy^2 = 1$ with square-free $D$), results of a more or less general nature were for a long time elusive. In 1887 Runge devised the general approach whose essence is described below (see also [145], p.262).

Equation (1.1) determines an algebraic function $y(x)$ which takes integral values at integer solutions of the equation. Suppose there are infinitely many solutions. One can find $y(x)$ numerically for sufficiently large $x$ by expansion in a power series about the point at infinity.

Let

$$F(x,y) = f_n(x,y) + f_{n-1}(x,y) + \ldots + f_0(x,y)$$

where $f_j(x,y)$ is a binary form of degree $j$. Put $x = t^{-1}$ and $y = st^{-1}$, and write

$$\begin{aligned} G(t,s) = t^n F(t^{-1}, st^{-1}) &= \\ &= t^n f_n(t^{-1}, st^{-1}) + t \cdot t^{n-1} f_{n-1}(t^{-1}, st^{-1}) + \ldots \\ &= g_n(s) + g_{n-1}(s)t + \cdots \end{aligned}$$

where $g_n(s)$, $g_{n-1}(s)$, $\ldots$ are polynomials in $s$. Suppose that $g_n(s) = f_n(1,s)$ has no multiple roots. The equation $G(t,s) = 0$ following from (1.1) defines $n$ power series expansions

$$s = \alpha + \alpha_0 t + \alpha_1 t^2 + \ldots ,$$

one for each root $\alpha$ of the polynomial $g_n(s)$, the numbers $\alpha_i$ being in the field $\mathbb{K} = \mathbb{Q}(\alpha)$. Consequently we have $n$ expansions

$$y = \alpha x + \alpha_0 + \alpha_1 x^{-1} + \dots \tag{1.2}$$

corresponding to the roots $\alpha$ of $g_n(s)$.

Let $\phi(x)$ denote one of the $n$ power series (1.2). The principal idea of Runge consists in a choice of integral polynomials $A_i(x)$, $(0 \leq i \leq n-1)$ of degree not exceeding some bound $h$, such that a power series expansion of the function

$$\Phi(x) = \sum_{i=0}^{n-1} A_i(x)\phi^i(x)$$

about the point at infinity has only negative powers of $x$:

$$\Phi(x) = \beta_1 x^{-1} + \beta_2 x^{-2} + \dots \tag{1.3}$$

When can this be done? Writing $\Phi(x)$ in the form

$$\Phi(x) = \sum_{j=-h-n+1}^{\infty} \beta_j x^{-j},$$

observe that each $\beta_j$ is a linear form in the unknown integer coefficients of the polynomials $A_0(x), \dots, A_{n-1}(x)$. We will have (1.3) when

$$\beta_j = 0 \qquad (j = -h-n+1, -h-n, \dots, 0). \tag{1.4}$$

Each $\beta_j$ lies in $\mathbb{K}$, and may therefore be represented by its coordinates with respect to a basis of $\mathbb{K}$ as a $\mathbb{Q}$-vector space. Then the system of equations (1.4) becomes a system of $d(h+n)$ linear homogeneous equations with rational coefficients, where $d = \deg \mathbb{K}$, in the $n(h+1)$ unknown integer coefficients of the polynomials $A_0(x), \dots, A_{n-1}(x)$. Provided $n(h+1) > d(h+n)$ we can guarantee the existence of a non-zero set of integers satisfying the system. If $d = n$ this cannot be done, but for $d < n$ it suffices to take $h = n^2 - n + 1$. Thus we can find a non-zero set of integral polynomials of degree not exceeding $n^2 - n + 1$ for which (1.3) will hold, provided that the polynomial $f_n(1, s)$ is reducible in $\mathbb{Q}[s]$.

We now substitute in (1.3) the integer values of $x$ for which there exists an integer $y$ satisfying (1.1) and (1.2). For such $x$, $y$, with $|x|$ sufficiently large, we obtain

$$\sum_{i=0}^{n-1} A_i(x) y^i = 0, \tag{1.5}$$

since it follows from (1.3) that $|\Phi(x)| < 1$ for sufficiently large $|x|$, and so $\Phi(x)$, being a rational integer, is zero. We have obtained an equation (1.5) which is independent of (1.1). The polynomial $F(x, y)$ is irreducible in $\mathbb{Q}[x, y]$ and its degree with respect to $y$ is $n$, while the left hand side of (1.5) has degree in $y$ not exceeding $n - 1$. Writing the resultant of these polynomials with respect to $y$, we obtain an equation only for $x$, which completes the proof of the finiteness of the number of solutions to (1.1) under the assumption that the polynomial $f_n(1,y)$ is reducible.

Clearly the above argument is effective, and may be used in concrete cases to determine all solutions of (1.1). Its further development yields very strong bounds on the solutions (such as a power of the height of $F(x,y)$).

Certainly the requirement that $f_n(1,y)$ be reducible is a serious restriction. Even the case $F(x,y) = f_n(x,y) + f_0(x,y)$, with $f_n$ irreducible, is of interest, being the problem of representation of numbers by irreducible binary forms. For $n = 2$ the finiteness or otherwise of the number of solutions is easily resolved, but even for $n = 3$ significant difficulties arise. The general case was solved by Thue, using a method which has influenced the development of the whole of this branch of number theory.

## 2. Liouville's Inequality; the Theorem and Method of Thue

In 1844 Liouville [128] observed that algebraic numbers do not admit 'very strong' approximation by rational numbers, and was thereby able to give the first construction of transcendental numbers. Since then the approximation estimate he obtained has been so frequently and widely applied that it has acquired a proper name: Liouville's Inequality.

Let $\alpha$ be a real algebraic number of degree $n \geq 2$ and let $p, q$ be integers. Then Liouville's inequality is

$$|\alpha - p/q| > c_1 q^{-n}, \tag{2.1}$$

where $c_1 = c_1(\alpha) > 0$ is a value depending explicitly on $\alpha$. The proof is immediate from the upper bound for the absolute value of $\mathrm{Nm}(\alpha q - p)$ and the observation that it is a non-zero rational number with denominator dividing $a^n$, where $a$ is an integer such that $a\alpha$ is an algebraic integer. For $n = 2$ it is impossible to improve on (2.1) by replacing $c_1$ by some positive function $\lambda(q)$ increasing monotonically to infinity, for it is known from the theory of continued fractions that, for any quadratic irrational $\alpha$, the reverse of (2.1) has infinitely many solutions in integers $p, q$ when $c_1$ is replaced by $\sqrt{5}$ (see [40], Ch. II). For $n \geq 3$,however, a sharpening of the (2.1) of the type

$$|\alpha - p/q| > \lambda(q)/q^n, \qquad \lambda(q) \uparrow \infty \tag{2.2}$$

is of great interest for the study of diophantine equations.

Indeed, let $f(x,y)$ be an integral irreducible binary form of degree $n \geq 3$, and suppose that $A \neq 0$ is an integer. If the inequality (2.1) admits a sharpening of the form (2.2) for some $\lambda(q)$, then the diophantine equation

$$f(x,y) = A \tag{2.3}$$

has only finitely many solutions.

If $f(x,1)$ is a polynomial without real roots, it is obvious that (2.3) has only a finite number of solutions. Suppose instead that $\alpha$ is a real root of $f(x,1)$ and $\alpha^{(i)}, i = 1, 2, \dots n$ its conjugates. It follows from (2.3) and $y \neq 0$ that

$$\prod_{i=1}^{n} |\alpha^{(i)} - x/y| = A/(|a||y|^n) \tag{2.4}$$

where $a$ is the leading coefficient of the polynomial $f(x,1)$. Assuming the equation (2.3) has integer solutions with arbitrarily large $|y|$ we see that the product on the left of (2.4) takes arbitrarily small values for solutions $x, y$ of (2.3). As all the $\alpha^{(i)}$ are different, $x/y$ must be correspondingly close to one of the real numbers $\alpha^{(i)}$, say $\alpha$.

Thus we obtain

$$|\alpha - x/y| < c_2/|y|^n$$

where $c_2$ depends only on $a$, $n$, and $\prod_{i \neq j} |\alpha^{(i)} - \alpha^{(j)}|^{-1} A$ (see Ch. IV, §1). Comparison of this inequality with (2.2) shows that $|y|$ cannot be arbitrarily large, and so the number of solutions of (2.3) is finite.

It is not difficult to see that the arguments are effective, and that an explicit bound can be constructed for solutions of (2.3) once an effective inequality (2.2) is known. The sharpening of the Liouville inequality (2.1), however, especially in effective form, proved to be very difficult.

In 1909 Thue published a proof [229] that

$$|\alpha - p/q| < q^{-\frac{n}{2}-1-\varepsilon} \tag{2.5}$$

has only finitely many solutions in integers $p, q > 0$ for all algebraic numbers $\alpha$ of degree $n \geq 3$ and any $\varepsilon > 0$. In essence, he obtained the inequality (2.2) with $\lambda(q)$ of the form $c_3 q^{\frac{1}{2}n-1-\varepsilon}$, where $c_3 > 0$ depends on $\alpha$ and $\varepsilon$. But Thue's arguments do not allow one to find a bound for the greatest $q$ satisfying (2.5), so it is impossible to exhibit the dependence of $c_3$ on $\alpha$ and $\varepsilon$, and so the bound for the number of solutions to (2.3) cannot be given in explicit form either: it is *ineffective*.

We shall show that the inequality (2.5) has just finitely many solutions following the arguments of Thue himself (see also [51]). Obviously, one may suppose that $(p,q) = 1$ in (2.5) and that $\alpha$ is an algebraic integer. Suppose that $h > 0$ is an integer, $\delta$ satisfies $0 < \delta < 1$, and

$$m = \left\lfloor \tfrac{1}{2}(n-2)(1+\delta)h \right\rfloor . \tag{2.6}$$

For each $h$ we will construct auxiliary polynomials $P(x)$, $Q(x)$ of minimal degree and height such that $P(x) - \alpha Q(x)$ is divisible by $(x-\alpha)^h$. In more detail, put

$$P(x) - \alpha Q(x) = (x-\alpha)^h \left\{ R_0 + R_1(x)\alpha + \ldots + R_{n-1}(x)\alpha^{n-1} \right\} \tag{2.7}$$

where the integral polynomials $R_0(x), \dots, R_{n-1}(x)$ are chosen so that their degrees do not exceed $m$ and not all of them are zero. Then we have $n(m+1)$