CAMBRIDGE TRACTS IN MATHEMATICS

General Editors

B. BOLLOBÁS, W. FULTON, A. KATOK, F. KIRWAN,
P. SARNAK, B. SIMON, B. TOTARO

**207 Auxiliary Polynomials in Number Theory**

CAMBRIDGE TRACTS IN MATHEMATICS

GENERAL EDITORS

B. BOLLOBÁS, W. FULTON, A. KATOK, F. KIRWAN,
P. SARNAK, B. SIMON, B. TOTARO

A complete list of books in the series can be found at www.cambridge.org/mathematics.
Recent titles include the following:

171. Orbifolds and Stringy Topology. By A. ADEM, J. LEIDA, and Y. RUAN
172. Rigid Cohomology. By B. LE STUM
173. Enumeration of Finite Groups. By S. R. BLACKBURN, P. M. NEUMANN, and G. VENKATARAMAN
174. Forcing Idealized. By J. ZAPLETAL
175. The Large Sieve and its Applications. By E. KOWALSKI
176. The Monster Group and Majorana Involutions. By A. A. IVANOV
177. A Higher-Dimensional Sieve Method. By H. G. DIAMOND, H. HALBERSTAM, and W. F. GALWAY
178. Analysis in Positive Characteristic. By A. N. KOCHUBEI
179. Dynamics of Linear Operators. By F. BAYART and É. MATHERON
180. Synthetic Geometry of Manifolds. By A. KOCK
181. Totally Positive Matrices. By A. PINKUS
182. Nonlinear Markov Processes and Kinetic Equations. By V. N. KOLOKOLTSOV
183. Period Domains over Finite and p-adic Fields. By J.-F. DAT, S. ORLIK, and M. RAPOPORT
184. Algebraic Theories. By J. ADÁMEK, J. ROSICKÝ, and E. M. VITALE
185. Rigidity in Higher Rank Abelian Group Actions I: Introduction and Cocycle Problem. By A. KATOK and V. NIŢIČĂ
186. Dimensions, Embeddings, and Attractors. By J. C. ROBINSON
187. Convexity: An Analytic Viewpoint. By B. SIMON
188. Modern Approaches to the Invariant Subspace Problem. By I. CHALENDAR and J. R. PARTINGTON
189. Nonlinear Perron-Frobenius Theory. By B. LEMMENS and R. NUSSBAUM
190. Jordan Structures in Geometry and Analysis. By C.-H. CHU
191. Malliavin Calculus for Lévy Processes and Infinite-Dimensional Brownian Motion. By H. OSSWALD
192. Normal Approximations with Malliavin Calculus. By I. NOURDIN and G. PECCATI
193. Distribution Modulo One and Diophantine Approximation. By Y. BUGEAUD
194. Mathematics of Two-Dimensional Turbulence. By S. KUKSIN and A. SHIRIKYAN
195. A Universal Construction for Groups Acting Freely on Real Trees. By I. CHISWELL and T. MÜLLER
196. The Theory of Hardy's Z-Function. By A. IVIĆ
197. Induced Representations of Locally Compact Groups. By E. KANIUTH and K. F. TAYLOR
198. Topics in Critical Point Theory. By K. PERERA and M. SCHECHTER
199. Combinatorics of Minuscule Representations. By R. M. GREEN
200. Singularities of the Minimal Model Program. By J. KOLLÁR
201. Coherence in Three-Dimensional Category Theory. By N. GURSKI
202. Canonical Ramsey Theory on Polish Spaces. By V. KANOVEI, M. SABOK, and J. ZAPLETAL
203. A Primer on the Dirichlet Space. By O. EL-FALLAH, K. KELLAY, J. MASHREGHI, and T. RANSFORD
204. Group Cohomology and Algebraic Cycles. By B. TOTARO
205. Ridge Functions. By A. PINKUS
206. Probability on Real Lie Algebras. By U. FRANZ and N. PRIVAULT
207. Auxiliary Polynomials in Number Theory. By D. MASSER

# Auxiliary Polynomials in Number Theory

DAVID MASSER
*University of Basle, Switzerland*

CAMBRIDGE
UNIVERSITY PRESS

CAMBRIDGE
UNIVERSITY PRESS

University Printing House, Cambridge CB2 8BS, United Kingdom

Cambridge University Press is part of the University of Cambridge.

It furthers the University's mission by disseminating knowledge in the pursuit of education, learning, and research at the highest international levels of excellence.

www.cambridge.org
Information on this title: www.cambridge.org/9781107061576



First published 2016

*A catalogue record for this publication is available from the British Library.*

*Library of Congress Cataloguing in Publication Data*
Names: Masser, David William, 1948–
Title: Auxiliary polynomials in number theory / David Masser, Universitat Basel, Switzerland.
Description: Cambridge : Cambridge University Press, 2016. | Series: Cambridge tracts in mathematics ; 207 | Includes bibliographical references and index.
Identifiers: LCCN 2015050947 | ISBN 9781107061576 (Hardback : alk. paper)
Subjects: LCSH: Number theory. | Polynomials.
Classification: LCC QA241 .M395 2016 | DDC 512.7/4–dc23 LC record available at http://lccn.loc.gov/2015050947

ISBN 978-1-107-06157-6 Hardback

# Contents

# Introduction

Ever since it was invented, arguably by Runge, the method of auxiliary polynomials has been vital to (and of unreasonable effectiveness in) the modern development of key aspects of number theory. The aim of this book is to give an account of the method in many of its forms, focusing almost exclusively on those polynomials which cannot be written down explicitly.

I well remember (standing in Heffers bookshop Cambridge around 1970) reading about this method in the foreword to Lang's book on transcendental numbers, and experiencing disbelief that anything so far-fetched could work at all. So I will not attempt any explanation at this point.

Instead, I (or from now on, the authorial we) treat the method as the union of its examples, and there is no shortage of these.

Here is the plan of this book (Mike Tyson said that everyone has a plan until you punch them in the face – then they don't have a plan). The general strategy is to present in each chapter an application of the method to a different sort of problem, often the simplest in its area. Then at the end of each chapter we give a brief account of subsequent developments in the area.

We start with a short Prologue (Chapter 1) where we show that the basic idea can be used in rather simple situations which have nothing to do with number theory.

Then in Chapter 2 we commence our diophantine considerations with a discussion of irrationality. We quickly dispose of the number $e$ by the standard truncation argument and we show also that $e$ is not a quadratic irrational. Here we meet a small problem, which can be rather quickly solved; however, it is typical of the problems that arise in later applications and in some examples its solution can be distinctly non-trivial. Thus Roth, in showing that irrational algebraic numbers cannot be approximated to within an order of $q^{-2-\epsilon}$ by rationals $p/q$, had to solve such a problem. The solution is called

Roth's Lemma, and it was certainly one of the achievements that gained him a Fields Medal. We do not prove Roth's Theorem here but we do treat Thue's Method in Chapter 12.

We postpone to Chapter 13 a proof that

$$e^{\alpha} = \sum_{k=0}^{\infty} \frac{\alpha^k}{k!} = 1 + \alpha + \frac{1}{2}\alpha^2 + \frac{1}{6}\alpha^3 + \frac{1}{24}\alpha^4 + \cdots$$

is irrational and even transcendental for all rational and even algebraic $\alpha \neq 0$, as this requires elements of algebraic number theory. Truncation gives only irrationality and that essentially only for $\alpha = 1, 2, 4$ (and slightly surprisingly $\alpha = \sqrt{2}$).

In the same Chapter 2 we construct our first auxiliary polynomial with a diophantine purpose: namely, to show that for any rational $\alpha \neq 0$ the classical series

$$\sum_{k=0}^{\infty} \frac{\alpha^k}{2^{k(k-1)/2}} = 1 + \alpha + \frac{1}{2}\alpha^2 + \frac{1}{8}\alpha^3 + \frac{1}{64}\alpha^4 + \cdots$$

is irrational. This is somewhat related to theta functions. Although it converges quite rapidly, the speed is also insufficient for mere truncation. The result itself is not so fundamental, but it provides a good introduction to the use of auxiliary polynomials; that used here is probably the simplest of its kind, and we calculate a few examples. One needs also some elementary complex analysis, which will be much developed later on.

In Chapter 3 we then progress to the similar but more elaborate Mahler's Method, still sticking just to irrationality; the results here are historically important and they led to the solution of the Mahler–Manin Conjecture and then to Nesterenko's Theorem on the algebraic independence of $\pi$ and $e^{\pi}$. The irrationality here will be generalized to full-blooded transcendence in a later chapter. Here we treat just

$$\sum_{k=0}^{\infty} \alpha^{2^k} = \alpha + \alpha^2 + \alpha^4 + \alpha^8 + \alpha^{16} + \cdots$$

for every rational $\alpha$ with $0 < |\alpha| < 1$. The proof is quite similar to that in Chapter 2 but a little more analysis is needed, and further the auxiliary polynomial is more complicated, in fact already of a fairly typical sort; still we calculate some more examples. Mahler's Method has been greatly developed and some recent applications refer to the famous Mandelbrot set. It also played a transient role in proving that the decimal digits of numbers like $\sqrt{2}$ cannot be generated by a finite automaton.

In Chapter 4 we prove that certain diophantine equations in two variables have at most finitely many solutions, using the auxiliary polynomial pioneered by Runge. The method enables all solutions to be found in principle. A typical example is that there are at most finitely many integers $x, y$ with

$$x(x^3 - 2y^3) = y.$$

Or, coming from Cassels's well-known result on the Catalan Equation recently solved completely by Mihăilescu, there are at most finitely many integers $x, y$ with $x^5 - y^7 = 1$ provided $y$ is not divisible by 5 (we do not prove Mihăilescu's Theorem here). Of course equations like

$$x^3 - 2y^3 = m$$

for fixed $m$ are more natural, and these will be considered in Chapter 12. For the proofs here, we need to know that the large complex solutions are given by Puiseux (or better Laurent) series. It seems that this is not so easy to find in the literature, especially regarding the crucial convergence properties, so we provide quite a few details.

Then in Chapter 5 we prove some results similar to the classical Hilbert Irreducibility Theorem, usually abbreviated to HIT, by using the machinery of the preceding chapter. They are not so general as HIT, but when they do work, they deliver more information. The results were first found by Sprindzhuk also using auxiliary polynomials, but in a more elaborate way. Nowadays this sort of thing can be done with heights machinery, but that is not so elementary. A typical example, related to that of the previous chapter, is that there are at most finitely many integers $y$ such that the polynomial

$$X(X^3 - 2y^3) - y$$

in $\mathbb{Q}[X]$ is reducible over the rationals, and in principle these can all be found. A literal application of HIT would show only that there are infinitely many rational $y$ such that the polynomial is not reducible. So sometimes we get a Strong Hilbert Irreducibility Theorem; but we refrain from abbreviating this. Here we need resultants; these can be found almost anywhere, but because we use them frequently in this book we provide a self-contained account.

In Chapter 6 we jump to a different topic. We prove that the number $N$ of points modulo a prime $p$ on an affine elliptic curve satisfies

$$|N - p| \le 8\sqrt{p};$$

this is slightly weaker than the classical result of Hasse involving $2\sqrt{p}$. The proof uses the simplest non-trivial example of the auxiliary polynomial introduced in a surprising way by Stepanov in 1969; here we attempt to motivate the

proof with the help of some easier intermediate results. Not even the definition of elliptic curve is needed here, let alone any properties. Thus all we do is count the integer solutions $(x, y)$ modulo $p$ of an equation $y^2 = x^3 + ax^2 + bx + c$ modulo $p$. There are many generalizations (and Schmidt wrote an entire book about them) but none has quite the same appeal. With rather little extra effort one can treat $y^2 = x^5 + \cdots$ and worse; in the geometric context this is far from simple because it would involve curves of genus 2 and worse.

In Chapter 7 we make another jump which seems even bigger, to the topic of exponential sums. The best known is Gauss's

$$\sum_{k=1}^{p} \exp\left(\frac{2\pi i k^2}{p}\right),$$

also for prime $p$, whose absolute value $p^{1/2}$ is much smaller than the number of its terms. One of these sums, due to Heilbronn, resisted for some time all efforts to prove its smallness until Heath-Brown in 1996 achieved this. His beautiful proof imitated Stepanov's auxiliary polynomial in a kind of analytic context involving a logarithm-like function. Some arguments had been anticipated by Mitkin in 1992. We give the details. Specifically

$$\left|\sum_{k=1}^{p} \exp\left(\frac{2\pi i k^p}{p^2}\right)\right| \le 4p^{11/12}.$$

As far as I know, these arguments have not been developed very far since then, despite some interesting features involving differential equations.

In Chapter 3 we proved the irrationality of the values $\mu$ of Mahler's series at non-zero rationals. Thus the quantity $|\mu - p/q|$ is positive for all integers $p$ and $q \ge 1$. A natural question is: "How small can this quantity get?" Indeed with an algebraic irrational in place of $\mu$ this question is fundamental in the theory of diophantine equations, as we will see in Chapter 12. Our answer in Chapter 8 requires refining the arguments of Chapter 3. There are two key steps. One is a "zero estimate" asserting that not too many things can vanish; such estimates play a major role in more recent developments. The other, more classical, is an estimate for the coefficients of the auxiliary polynomial; this involves the famous Siegel Lemma, which will be used over and over again in the sequel. We also make a simple application of the maximum modulus principle for analytic functions. This too will be used frequently later, under the popular name of the Schwarz Lemma. In this way we will prove that there exist $c = c(\mu) > 0$ and $\kappa = \kappa(\mu)$ such that

$$\left|\mu - \frac{p}{q}\right| \ge \frac{c}{q^\kappa}.$$

For example with $\mu = \sum_{k=0}^{\infty}(2/3)^{2^k}$ we can take $\kappa = 77$.

There is a famous result of Pólya on entire functions mapping the natural numbers to the rational integers; this may have influenced Gelfond in his pioneering work on the transcendence of $\alpha^\beta$ (see Chapter 19). Pólya's original proof used interpolation formulae and gave the best possible constant. Much later Waldschmidt gave a version by auxiliary polynomials, which sadly gives a worse constant. The proof is nevertheless illuminating; it needs binomial coefficients to avoid factorials, one of the key ideas in Thue's famous proof (see Chapter 12). More precisely, we show in Chapter 9 that an entire function $f$ with

$$f(0), f(1), f(2), \ldots, f(n), \ldots$$

all in $\mathbb{Z}$ must be a polynomial if $|f(z)|$ grows of order at most $C^{|z|}$ for a certain $C > 1$. Pólya could take any $C < 2$; and the standard example $2^z$ shows that nothing better is possible. Or reformulated: if a non-polynomial entire function $f$ has this growth, then at least one of $f(0), f(1), f(2), \ldots$ must be non-integral. Gelfond's step from non-integrality to transcendence needed many more ideas, all of which will be developed in this book.

The rather natural generalization to the Gaussian integers $\mathbb{G} = \mathbb{Z} + \mathbb{Z}i$ with $f$ mapping $\mathbb{G}$ into itself also played a similar historical role; for example it probably directly inspired Gelfond's proof of the transcendence of $e^\pi$. But the best possible constant did not appear until a relatively recent paper of Gramain; paradoxically enough, his proof involves an auxiliary polynomial (or better an auxiliary function). More precisely, $f$ itself must be a polynomial if $|f(z)|$ now grows of order at most $C^{|z|^2}$ for a certain $C > 1$. Gelfond considered this problem too, and obtained the notorious value

$$C = \exp\left(\frac{\pi}{2(1+\exp(164/\pi))^2}\right) < 1 + 10^{-45}$$

(modestly not mentioned in his book). In the late 1970s, I obtained a constant, extremely difficult to compute, which later turned out to be about 1.181; and I conjectured that the best possible constant was $\exp(\frac{\pi}{2e})$ about 1.782. This Gramain proved, and so do we in Chapter 10.

In Chapter 11 we present our first transcendence result. We extend Mahler's Method in Chapter 3 to prove the transcendence of his $\sum_{k=0}^{\infty}\alpha^{2^k}$ for all algebraic $\alpha$ with $0 < |\alpha| < 1$. That is apparently how he tested his recovery while convalescing at home from an illness. No more ideas are needed, but to go beyond irrationality requires some rudimentary notion of "size" of an algebraic number, with some sort of "Liouville estimate". This sort of technicality is fundamental to all transcendence proofs. The concept will be developed later

into the more sophisticated "height", which will then be studied for its own sake, for example with reference to Lehmer's Question of 1933 in connexion with factorization problems.

At last in Chapter 12 we prove the famous Thue improvement of Liouville's classical result. The proofs here start getting more elaborate, and another key element is dealing with the dangerously heavy factorials that threaten to sink the method; however this problem has been solved in Chapter 9. Yet another feature is a simple form of zero estimate. These have proved crucial in later developments involving Roth, Schmidt, Schlickewei, and others. More precisely, given any algebraic number $\alpha$ of degree $d \geq 3$ and any $\kappa > \frac{d}{2} + 1$, we show that there is a positive constant $c = c(\alpha, \kappa)$ such that

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

for all integers $p$ and $q \geq 1$. The Liouville result was for $\kappa = d$, and the later Roth estimate was for any $\kappa > 2$. Here we try to break the proof into molecules, and we also speculate on how Thue may have arrived at his proof; there are interesting connexions with Newton's Method in numerical analysis and later improvements by Halley and others. We also give the applications to diophantine equations. Here we encounter the uncomfortable phenomenon of ineffectivity for the first time.

Then in Chapter 13, using the machinery of the previous chapter, we prove the Hermite–Lindemann result on the transcendence of the values of the exponential function at algebraic numbers; thus $e^\alpha$ is transcendental for every algebraic $\alpha \neq 0$. Our proof is a kind of *ad hoc* development of the auxiliary polynomial techniques introduced so far; we have by now illustrated so many of these techniques that several proofs are available. We choose the one most suited for generalization to the Schneider–Lang Theorem later on in Chapter 19.

Chapter 14 is where we develop the size in Chapter 11 to the absolute height $H(\alpha) \geq 1$ or the logarithmic version $h(\alpha) = \log H(\alpha) \geq 0$. This is rather easy to define, but to establish properties like $H(\alpha^2) = H(\alpha)^2$, we need quite a bit of algebraic number theory, and we will sketch the details. The motivation is two-fold: first, the results of the next two chapters are about heights *per se*, and second, the proof of the later Schneider–Lang result then becomes fairly streamlined. We also give a version of the Siegel Lemma in the heights language. This requires essentially defining the height of a vector $(\alpha_1, \ldots, \alpha_n)$ of algebraic numbers. To break the monotony, we prove on the way some easy results on lower and upper bounds for heights that have led to some lively modern developments.

Then in Chapter 15 we prove Bilu's Theorem on the distribution of the conjugates of an algebraic number, using an auxiliary polynomial due to Mignotte as well as the Siegel Lemma from the previous chapter. As a matter of fact, our version is completely explicit numerically. But there is a problem: this explicitness is based on the Erdős–Turán Theorem, and there seems to be no easy proof of that. So at this point the book is definitely not self-contained; however we find this didactically permissible, as the present chapter serves as a natural springboard for the next one, and Bilu's Theorem is not further used in the book. More precisely, if $\alpha$ is an algebraic number of degree $d$ and absolute logarithmic height $h$, we show that the number $n$ of its conjugates in any sector of angle $\theta$ based at the origin satisfies

$$\left| n - \frac{\theta}{2\pi} d \right| \leq 24(d^{2/3}(\log 2d)^{1/3} + dh^{1/3}).$$

That $n$ is asymptotically $\frac{\theta}{2\pi}d$ as $h \to 0$ is the main content of Bilu's result (which is expressed more felicitously in terms of weak approximation).

Then in Chapter 16 using the machinery developed in the previous chapter, we prove up to logarithms the famous Dobrowolski Theorem, which is to this day the best approach to the classical Lehmer Question, using essentially the original auxiliary polynomial. The result is exceptionally useful and, as far as I know, none of the applications actually need the logarithms. Providing the best known logarithms is an exercise on the Prime Number Theorem, which is carried out in several books. Thus we prove here that for any $\kappa > 1$ there is a positive constant $c = c(\kappa)$ such that every non-zero algebraic $\alpha \neq 0$ of degree $d$ which is not a root of unity satisfies

$$h(\alpha) \geq \frac{c}{d^\kappa}.$$

Admittedly there are quicker proofs without auxiliary polynomials, but these don't generalize to the higher dimensional results such as the Amoroso–David Theorem that are very important today in diophantine geometry.

In Chapter 17 we restore some symmetry by giving a non-trivial height upper bound. This concerns the algebraic numbers $\alpha$ with $\alpha^n + (1-\alpha)^n = 1$ for some integer $n \geq 2$. In a relatively recent investigation connected with irreducibility, Beukers showed that $H(\alpha) \leq 216$. His proof used hypergeometric functions. Using instead the powerful method of auxiliary polynomials, we get $H(\alpha) \leq 10^{120}$ (in the style of Stephen Leacock "ten years ago the deficit on my farm was about a hundred dollars; but by well-designed capital expenditure, by drainage and greater attention to detail, I have got it into the thousands"). However this method generalizes considerably, as current work of Amoroso, Zannier and the author shows.

In Chapter 18 we use some of the ideas developed so far to give a generalization to algebraic points of the 1989 Bombieri–Pila Theorem on counting rational points on analytic curves. The original proof, although not fundamentally different from ours, is based on identities related to the confluent Lagrange Interpolation Formulae and not on an auxiliary polynomial. Such counting results (usually in higher dimensions) are nowadays being applied to prove a variety of special cases of the general Zilber–Pink Conjectures about unlikely intersections. We will prove something implying the following. Let $f$ be a transcendental function analytic on an open set containing the real interval $[0, 1]$. Then for any $\epsilon > 0$ there exists $c = c(f, \epsilon)$ such that, for every positive integer $n$, at most $cn^{\epsilon}$ of the values

$$f(0), f\left(\frac{1}{n}\right), f\left(\frac{2}{n}\right), \ldots, f(1)$$

are in $\mathbb{Z}/n$. This vaguely resembles the reformulation of Pólya's Theorem.

Then in Chapter 19 we prove the famous Schneider–Lang Theorem, which includes Hermite–Lindemann in Chapter 13 as well as several other things involving elliptic and abelian functions. Thanks to the preceding chapters the proof is now reasonably smooth. It is a natural climax to the book; however the next chapter follows on quite naturally, and so does the one after that. Thus we prove the Gelfond–Schneider Theorem on the transcendence of $\alpha^{\beta} = \exp(\beta \log \alpha)$ whenever $\alpha \neq 0$ and irrational $\beta$ are algebraic, which includes the transcendence of $2^{\sqrt{2}}$ as specified by Hilbert in his Seventh Problem. A key technical trick is the use of "large radius" in the Schwarz Lemma.

In Chapter 20 we systematically consider the elliptic analogues, motivated partly by the need to prove the transcendence of integrals like

$$\int_0^1 \frac{\mathrm{d}X}{\sqrt{X - X^3}}, \quad \int_4^5 \frac{(X-8)\mathrm{d}X}{\sqrt{X^3 - 7X + 6}}.$$

The results involve a Weierstrass function $\wp(z)$ with invariants $g_2, g_3$ that are themselves algebraic; the analogue of Hermite–Lindemann then asserts the transcendence of $\wp(\alpha)$ for any algebraic $\alpha \neq 0$. Already the elliptic analogue of Gelfond–Schneider has consequences for the modular function $j(\tau)$ defined on the upper half-plane: namely that $j(\alpha)$ is transcendental whenever $\alpha$ is algebraic but not quadratic; this we postpone to the next chapter. But as Schneider discovered, there are several other interesting consequences; and even he overlooked one of them. This chapter is the longest in the book, due to our supplying the main details for the proofs of most of these consequences. It might get shorter if we could use facts about commutative group varieties, but

that would introduce too much algebraic geometry not in the elementary spirit of the book.

In 1969 Mahler conjectured that the alternative modular function

$$J(q) = q^{-1} + 744 + 196884q + 21493760q^2 + 864299970q^3 + 20245856256q^4 + \cdots$$

(the pattern of coefficients is quite self-evident), defined for all $q$ in the unit disc, takes transcendental values at non-zero algebraic $q$. In 1996 Barré, Diaz, Gramain and Philippon proved this using an auxiliary polynomial directly on $J$ itself. This was not only the first auxiliary polynomial of its kind (as Schneider had wanted many years ago in his Second Problem), but it led soon afterwards to Nesterenko's unexpected breakthrough implying the algebraic independence of $\pi$ and $e^\pi$. This is a most attractive area where aspects of elliptic, modular and exponential functions blend into each other. We give a proof of Mahler's Conjecture in Chapter 21, after deducing the analogous result for $j(\tau) = J(e^{2\pi i\tau})$ from the results of the previous chapter.

Up to now we never discussed problems of algebraic independence. Maybe the reader's curiosity for this topic has been awakened at the end of the previous chapter, and now she gets a classical example. After the famous Lindemann–Weierstrass result (not covered in this book), which was generalized to $E$-functions by Siegel and Shidlovsky (likewise not here), the most spectacular was the algebraic independence of $\alpha^\beta$ and $\alpha^{\beta^2}$, for algebraic $\alpha \neq 0$ and cubic $\beta$, due to Gelfond in 1949. But as a lot of the machinery is already available, our proof in Chapter 22 will not be too long. Here too one needs "large radius".

Finally in an Appendix we prove exotic height results like

$$h\left(\frac{3\xi - 4\sqrt{\xi^3 + 3\xi + 4} + 8}{\xi^2}\right) \leq h(\xi) + 10000(\sqrt{h(\xi)} + 1)$$

where a crude estimate would give at least $2h(\xi)$ on the right-hand side. Indeed if we replace 8 in the numerator by 7 this is unavoidable. The square root here, traditionally associated with the quadratic nature of Néron–Tate heights on abelian varieties, is actually needed.

Let us mention here yet another use for auxiliary polynomials: to show that certain algebraic numbers arising from commutative group varieties have "large degree". It is well-known that the root of unity $e^{2\pi i/n}$ has degree $\phi(n)$ the Euler $\phi$-function, and also that for any $\theta < 1$ there is a positive constant $c$, of course effectively computable, with $\phi(n) \geq cn^\theta$. By a famous result of Serre the elliptic analogue has any $\theta < 2$, but only recently has this been made effective, in an elaborate proof involving, among other things,

isogeny estimates. Using an auxiliary polynomial directly, in the functions $\wp(z), \wp(Nz)$ which are "almost algebraically independent", one can quickly obtain an effective lower bound for any $\theta < 1$. Furthermore this method works also for abelian varieties, where the analogue of Serre's Theorem is still not yet fully known. The resulting estimates have recently been very useful in problems of unlikely intersections. We omitted any detailed account, first for lack of space and second because one needs more theory, such as Néron–Tate heights. See Masser (1977) and also Appendix D of Zannier (2012). However in Exercise 14.92 we sketch how the lower bound $cn/\log n$ can be obtained in the cyclotomic case.

The reader will observe that the auxiliary polynomial usually operates in a proof by contradiction. So this book is mostly about things that don't exist! With Woody Allen we may hate reality but it's still the best place to get a decent steak. Or we may think of the Cape Town telephone company error message "the number that you have called does not exist".

The pleasant task of collecting together all these applications of auxiliary polynomials has resulted in some features that may not be familiar to all experts.

Thus I am not sure if Theorem 5.1 in Chapter 5 appears explicitly in the literature. In Chapter 6 the warm-up before the proof of Theorem 6.1 may not have appeared before in this form. In Chapter 7 the proof of Lemma 7.3 is new, although it proceeds on well-known general principles. The (rather easy) estimate (8.7) of Chapter 8 is probably new. In Chapter 10 the Proposition 10.4 might possibly be useful in other contexts. In Chapter 12 it is indeed I who must accept full responsibility for the attempt to explain the proof of Theorem 12.1 in terms of numerical analysis; also the Proposition 12.2, although known to some experts, may not have appeared explicitly before. Our explicit estimate in Theorem 15.2 of Chapter 15 could be new, although its shape is fairly well-known. Some of the preliminary discussion in Chapter 16 may not be familiar. The method introduced in Chapter 17 is new, due to Amoroso, Zannier and myself. In Chapter 18 the main result Theorem 18.2 for $\mathbb{Q}(i)$ is not in the published work that I have seen, although here too its shape for $\mathbb{Q}$ is fairly well-known. Lemma 20.7 from Chapter 20 might look familiar, but it is not; also some of the details towards the end of this chapter have never appeared in print, although this may well be due to the alternative approach, more conceptual to some, through group varieties. In particular the proof of Theorem 20.11 might well be a "desperately-needed gap in the literature". Here also the (again rather easy) remark about the gamma function is new. And in Chapter 21 the Lemma 21.8 enables us to avoid an appeal to certain estimates for coefficients of modular transformation polynomials, whose (non-classical) proofs are somewhat

elaborate. In Chapter 22 the proof of Proposition 22.5 is a small variation of a proof that I have seen. Finally in the Appendix the Theorem A.1, although presented only for a particular example, is also new, arising from the above work of Amoroso, Zannier and myself.

What are the prerequisites for a happy reading of this book? The first thirteen chapters could be understood by third-year university students or good second-year students (and indeed in 2013/2014 they were – and I thank this class, especially Gabriel Dill, who examined with a fine-toothed comb the first ten, although I may well have invented new mistakes during revision). The proofs are elementary (but that does not always imply that they are easy). Here there are elements of algebra such as the concept of transcendence, the fact that $\mathbb{Z}[X]$ is a unique factorization domain, or the integral closure of a ring $R$ in a larger ring $S$ (which I like to denote by $R_S$); elements of analysis such as order of vanishing, Cauchy's Theorem or the Maximum Modulus Principle; and elements of algebraic number theory such as field embeddings, conjugates or rings of integers. There is a jump at Chapter 14, where we need slightly more advanced algebraic number theory, which we explain without full proofs, freely using concepts like prime ideals and valuations. This enables us to get all the way to Chapter 20, where we then need some theory of elliptic functions, which again we explain without full proofs. Similarly in Chapter 21 we need some theory of modular functions. Finally in Chapter 22 we need a bit about transcendence degree. By contrast in the Appendix, although it has a considerable whiff of diophantine geometry, we develop from scratch the rudiments of algebraic curve theory that we need. And oh yes, it will be good to bear in mind that our

$$\mathbb{N} = \{1, 2, 3, \ldots\}$$

does not contain 0 as it might in some other cultures. But $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ and the fields $\mathbb{F}_p = \{0, 1, \ldots, p-1\}$ are unambiguous.

And what about the exercises? These are at the end of each chapter, where they are divided into two parts by a starred line. Those above the line need only the prerequisites above and what's in the book so far, and they are essentially what were fed to students as homework reinforcing the lectures. Those below the line go further, and sometimes need extra knowledge; they are of varying levels of difficulty, sometimes hinted at. Concerning the lectures themselves, there are many possibilities; for example I covered Chapters 1, 2, 3, 4, 5 together with some algebraic number theory in a single semester, then followed up with Chapters 6, 8, 9, 11, 12, 13 and more algebraic number theory, and so was able to start a third semester with Chapter 14 in detail, then Chapters 15, 16, 18, 19 and bits of Chapter 20.

There is also a bibliography, but this has no pretence of being comprehensive. Instead I have tried to restrict it to books, especially those that give a good overview of the subsequent development of some of the topics treated here; but I have also included some key original papers.

I conjecture, but have no time to prove, that every mathematics book with at least 100 pages contains at least one misprint (possibly apart from those that have gone through several editions – however in a 2008 seminar we did find a mistake in Landau's "Elementary Number Theory" (Chelsea 1958), despite the author, according to Littlewood, reading proof sheets seven times, once for each sort of error – curiously we could not find it again later, this "Lost Mistake"). Boas has a conjecture that is shockingly stronger, and (continued p. 94).

The book you are now reading is certainly no countexerample, and I apologize in advance for my misprints, howlers and blunders (and my King Charles's Head of continued fractions). In fact I was once thanked in print by a non-English author for "teaching him mistakes". I hope to be able to pass on these skills to my readers.

And also to convey to them the joys of "doing transcendence" rather than merely "doing mathematics".

I gladly express my great gratitude to David Tranah of Cambridge University Press, for his warm initial encouragement to write the book, for his gentle reminders about actually writing it, and, once I gave in and started in earnest, for his regular enquiries about its progress and his rapid and detailed answers to my many questions.