Saradha Natarajan
Ravindranathan Thangadurai

Pillars of Transcendental Number Theory

Springer

Pillars of Transcendental Number Theory

This picture is the great corridor at Rameshwaram Temple, Tamilnadu. The picture is taken from the following url address: https://commons.wikimedia.org/wiki/File:Grand_corridor,_rameshwaram_temple,tamilnadu_-_panoramio.jpg. Our thanks to Mr. Rajaraman Sundaram who has taken the photograph and made available for public in the above website

Saradha Natarajan · Ravindranathan Thangadurai

Pillars of Transcendental Number Theory

Springer

Saradha Natarajan
DAE Centre for Excellence
in Basic Sciences
University of Mumbai
Mumbai, Maharashtra, India

Ravindranathan Thangadurai
Department of Mathematics
Harish-Chandra Research Institute
Prayagraj, Uttar Pradesh, India

ISBN 978-981-15-4154-4 ISBN 978-981-15-4155-1 (eBook)
https://doi.org/10.1007/978-981-15-4155-1

This Springer imprint is published by the registered company Springer Nature Singapore Pte Ltd.
The registered company address is: 152 Beach Road, #21-01/04 Gateway East, Singapore 189721, Singapore

I seem to have been only like a boy playing on the seashore, and diverting myself in now and then finding a smoother pebble or a prettier shell than ordinary, whilst the great ocean of truth lay all undiscovered before me

—Isaac Newton

Dedicated

To

Our families

Preface

Since the proof of Hermite in 1873 on the transcendence of the classical constant e, the theory of transcendence has evolved as a well-developed subject due to the contributions of many mathematicians like Lindemann, Thue, Siegel, Gelfond, Schneider, Roth and others. Baker's work on linear forms in logarithms from 1965 to 1970 gave an impetus to the subject. The years that followed saw a resurgence of the subject. Several improvements were made in the lower bound estimates for linear forms in logarithms by Baker himself, Waldschmidt, Shorey and many others. These improved bounds have a wide number of *effective* applications in Diophantine equations, class number problems, powers in recurrence sequences, etc. Numerous papers have been written and are still being written using the theory of linear forms. The theory is a gold mine for researchers. There are several mathematicians all around the world who have made and are still making important contributions to this wonderful subject. We have mentioned only very few names and fewer results to keep the book as simple as possible.

There are a handful of books written on the theory of linear forms and its applications beginning with the book of Baker [1]. Some of the other books are by Waldschmidt [2], Shorey & Tijdeman [3], Baker & Wüstholz [4], Nesterenko [5] and Ram Murty & Rath [6].

With the ever-growing applications, it becomes important for any student who wants to work in this area, to know the proofs of Baker's original results. For this purpose, the only available sources are either Baker's book or his original papers or some online notes.

One of our primary aims of writing this book is to present Baker's original results in a way, suitable for students of postgraduate or first-year Ph.D. level. We intend to keep the exposition simple and easily accessible.

This book will begin with some classical results like the transcendence of e,π and Hermite–Lindemann–Weierstrass theorem. Our proof of the Gelfond–Schneider theorem is based on Siegel's method. A new feature here is that we will be showing some well-known results of Ramachandra, which are not widely known. Gelfond–Schneider theorem and many other interesting results will be derived from his results.

An important area, which got an impetus due to an ingenious method initiated by Thue in 1909, was *Diophantine Approximation*. This was developed by Siegel, Dyson, Gelfond and finally Roth, in 1955, obtained the best possible result for the approximation of an algebraic number by a rational. This result is now known as Thue–Siegel–Roth theorem. This theorem is an important pillar in this subject. The proof of Roth's theorem can be found in Schmidt [7]. There are a few other books which outline the proof of Roth's theorem. We will give proofs of theorems of Thue, improvement by Siegel and the theorem of Roth in this book. We will follow the original paper of Roth [8] (and [9]) for the proof of his theorem.

When students see all the three proofs in one place, they can understand how the ideas developed. Our aim is not only to give the proofs of the theorems, but to illustrate the *ineffectiveness* of these theorems with the *effectiveness* of Baker's result in solving Diophantine equations. Thue's equations have attracted a lot of attention lately. There are computational programs developed, by which, nowadays it is a routine matter to solve a Thue's equation. For any student who wants to work in this and allied areas, this is a prerequisite.

Another important pillar in this subject is Schmidt's subspace theorem. This is a multidimensional analogue of Roth's theorem. Of late, many interesting applications of subspace theorem are being discovered. Although we will not be able to give the proof of this theorem, we will illustrate the theorem with some applications including a recent one.

Each chapter will conclude with a few problems in the form of Exercise and some interesting information as Notes. We do not intend to be exhaustive in both Exercise and Notes. These are meant to infuse and instil curiosity for the reader.

Our aim is to bring important theorems of transcendence theory under one roof so that the subject can be taught as a well-knit graduate course. The style will be classical, simple and friendly to students. Postgraduate and Ph.D. students of pure mathematics can be benefited by a course based on this book. It will be a good collection in any pure mathematician's library and can use this for teaching a course in transcendence. As the book will be self-contained, the need to refer to other books will be minimal. A basic course in algebraic number theory [10], real and complex analysis [11, 12] will be required for any reader of this book.

The first author would like to thank the Indian National Science Academy for awarding her Senior Scientist Fellowship and DAE Centre for Excellence in Basic Sciences, University of Mumbai, for providing facilities. The second author is thankful to Harish-Chandra Research Institute for the excellent environment which helped in writing the book, and also he is thankful to Dr. Veekesh Kumar and Ms. Bidisha Roy for going through some chapters of this book in the first draft and for suggesting some of the exercises.

Mumbai, India — Saradha Natarajan
Prayagraj, India — Ravindranathan Thangadurai

References

1. A. Baker, *Transcendental Number Theory* (Cambridge Tracts, 1975) (Preface, Chapter 7 and Chapter 8).
2. M. Waldschmidt, *Nombres Transcendants* (Springer-Verlag, 1974) (Preface and Chapter 4).
3. T.N. Shorey, R. Tijdeman, *Exponential Diophantine Equations* (Cambridge Tracts, 1986 and re-printed in 2008) (Preface and Chapter 7).
4. A. Baker, G. Wüstholz, *Logarithmic Forms and Diophantine Geometry* (Cambridge Tracts, 2007) (Preface and Chapter 7).
5. Y.V. Nesterenko, *Algebraic Independence*, vol. 14 (Tata Institute of Fundamental Research Publications, 2008), 157pp (Preface, Chapter 2 and Chapter 3).
6. M. Ram Murty, P. Rath, *Transcendental Numbers* (Springer, 2014), 217pp (Preface, Chapter 2, Chapter 4 and Chapter 7).
7. W.M. Schmidt, *Diophantine Aproximation*, vol. 785 (Springer-Verlag LNM, Berlin-Heidelberg, 1980) (Preface and Chapter 9).
8. K.F. Roth, *Rational Approximations to Algebraic Numbers*. Mathematika **2**, 1–20 (1955); *Corrigendum* **2** (1955), p. 168. (Preface and Chapter 6).
9. W.J. LeVeque, *Topics in Number Theory, Vol I and II* (Dover Publication Inc, New York, 1984) (Preface and Chapter 6).
10. S. Lang, *Algebraic Number Theory*, vol. 110, 2nd edn. Graduate Texts in Mathematics (Springer-Verlag, New York, 1994) (Preface and Chapter 1).
11. T.M. Apostol, *Mathematical Analysis: A Modern Approach to Advanced Calculus* (Addison-Wesley Publishing Company, Inc., Reading, Mass., 1957) (Preface).
12. W. Rudin, *Real and Complex Analysis*, 3rd edn (McGraw-Hill Book Co., New York, 1987) (Preface).

Contents

About the Authors

Saradha Natarajan is an INSA Senior Scientist at the DAE Center for Excellence in Basic Sciences at the University of Mumbai, India, and elected fellow of the Indian National Science Academy (INSA). Earlier, she was Professor of Mathematics at the Tata Institute of Fundamental Research, Mumbai, India, until 2016. She earned her Ph.D. in 1983 under the guidance of Prof. T. S. Bhanumurthy from the Ramanujan Institute for Advanced Study in Mathematics, University of Madras, Chennai. She was a postdoctoral fellow at Concordia University, Canada; Macquarie University, Australia; and National Board of Higher Mathematics (NBHM), India.

Her area of specialization is number theory, in general, and transcendental number theory and Diophantine equations, in particular. She has published several papers in international journals of repute and has collaborated with many mathematicians both in India and abroad. Several students have completed their Ph.D. under her supervision. She has travelled extensively and given invited talks and lectures at national and international seminars and conferences. Professor Natarajan has made substantial contributions to the conjectures of Erdos on perfect powers in arithmetic progressions, where combinatorial and computational methods, linear forms in logarithms and modular method are combined. She also has made significant contributions to Thue equations and Diophantine approximations, especially towards conjectures of Bombieri, Mueller and Schmidt on number of solutions of Thue inequalities for forms in terms of number of non-zero coefficients of the form. In the area of transcendence, she has obtained best possible simultaneous approximation measures for values of exponential function and Weierstrass elliptic function. Further, significant lower bounds were shown for the Ramanujan tau-function for almost all primes p.

Ravindranathan Thangadurai is Professor at Harish-Chandra Research Institute, Prayagraj, India. He earned his Ph.D. in Combinatorial Number Theory in 1999 from the Mehta Research Institute for Mathematics and Theoretical Physics, Allahabad (now Harish-Chandra Research Institute, Prayagraj) under the

supervision of Prof. S. D. Adhikari. He spent two years as a postdoc at the Institute of Mathematical Sciences, Chennai, India, and two years at Indian Statistical Institute, Kolkata, India.

His areas of research include analytic, combinatorial and transcendental number theory, specifically, major contributions in the area of zerosum problems in finite abelian groups, distribution of residues modulo p, Liouville numbers and Schanuel's conjecture in transcendental number theory. He has collaborated with reputed mathematicians and his research articles have been published journals of repute. He has computed the exact values of Olson's constant and Alon–Dubiner constant for subsets for the group. He proved a conjecture of Schmid and Zhuang for large class of finite abelian p-groups and the current best known upper bound for Davenport's constant for a general finite abelian group. He has also made a major contribution to the theory of distribution of particular type of elements (specially, quadratic non-residues but not a primitive root) of residues modulo p. He has proved a strong form of Schanuel's conjecture in transcendental number theory for many n-tuples.

Symbols

$\mathbb{N}$	Positive rational integers
$\mathbb{Z}$	Ring of rational integers
$\mathbb{Q}$	Field of rational numbers
$\mathbb{R}$	Field of reals
$\mathbb{C}$	Field of complex numbers
$\mathbb{A}$	Field of algebraic numbers
$\mathcal{K}$	Number field
$\mathcal{O}_{\mathcal{K}}$	Ring of integers of $\mathcal{K}$
$\mathcal{O}_{\mathcal{K}}^*$	Group of units of $\mathcal{O}_{\mathcal{K}}$
$\mathcal{N}(\alpha)$	Norm of α over $\mathbb{Q}$ with respect to $\mathbb{Q}(\alpha)$
$\mathcal{N}_{\mathcal{K}/\mathbb{Q}}(\alpha)$	norm of α over $\mathbb{Q}$ with respect to $\mathcal{K}$
$\mathbf{F}[X]$	Ring of polynomials in X with coefficients in $\mathbf{F}$
$\mathbf{F}[X_1, \ldots, X_n]$	Ring of polynomials in $X_1, \ldots, X_n$ with coefficients in $\mathbf{F}$
$\mathcal{K}[[z]]$	Ring of power series with coefficients in $\mathcal{K}$
$[x]$	Integral part of real number x
$\{x\}$	Fractional part of real number x
$\|\|x\|\|$	Distance of real number x to the nearest integer
$\Re(z)$	Real part of z
$\Im(z)$	Imaginary part of z
$H(P)$	Height of a polynomial P
$h(\alpha)$	Height of an algebraic number α
$\lceil \alpha \rceil$	House of an algebraic number α
$d(\alpha)$	Denominator of an algebraic number α
$s(\alpha)$	Size of an algebraic number α
$h^\circ(\alpha)$	Absolute logarithmic height of an algebraic number α

Chapter 1
Preliminaries

The shell must break before the bird can fly

—Tennyson

In this chapter, we collect some basic results which will be used in the ensuing chapters.

While looking for the transcendence nature of values of some classical functions, it is apriori imperative to check if the given functions are transcendental functions or algebraically independent functions. In Sect. 1.1, we show the algebraic independence of the pairs of functions (z, e^{az}), (e^z, e^{az}) and $(\wp(z), \wp^*(z))$ where $0 \neq a \in \mathbb{C}$, $\wp$ and $\wp^*$ are Weierstrass elliptic functions.

Section 1.2 deals with the Gauss's lemma on primitive polynomials and factorisation of multi-variable polynomials.

In Sect. 1.3, we collect some basic properties of algebraic numbers and state Dirichlet's Unit theorem.

We give a criterion for linear independence of functions of single and several variables in terms of Wronskians in Sect. 1.4. In the multi-variable case, the notion of generalised Wronskian was introduced by Roth while proving his famous result on the approximation of an algebraic number by rationals. Their properties are explained in Lemmas 1.4.2 and 1.4.3. These are of independent interest also.

1.1 Algebraic Independence of Functions

Let $f_1, f_2, \ldots, f_\ell$ be complex functions defined on a field $\mathcal{K} \subset \mathbb{C}$. We say these functions are *algebraically independent over* $\mathcal{K}$ (respectively, *linearly independent over* $\mathcal{K}$), if for every non-zero polynomial $P(x_1, \ldots, x_\ell) \in \mathcal{K}[x_1, \ldots, x_\ell]$ (respectively, non-zero linear polynomial), there exists $z_0 \in \mathcal{K}$ such that the complex number

S. Natarajan and R. Thangadurai, *Pillars of Transcendental Number Theory*,
https://doi.org/10.1007/978-981-15-4155-1_1

$P(f_1(z_0), \ldots, f_\ell(z_0)) \neq 0$. When $\ell = 1$, we say the function f_1 is *transcendental over* $\mathcal{K}$.

Let $\rho > 0$ be a real number. We say that an entire function f is of *order* ρ if there exists an absolute constant $C > 0$ such that

$$|f|_R = \max_{|z|=R} |f(z)| \leq C^{R^\rho} \text{ for } R \to \infty.$$

For example, any polynomial $P(z) \in \mathbb{C}[z]$ is of order 0 while e^z has order 1. This notion is extended to meromorphic functions as follows. A meromorphic function is said to be of *order* ρ if it is the quotient of two entire functions of order $\leq \rho$. For example, the Weierstrass elliptic function $\wp(z)$ is known to be the quotient of entire functions of order 2. Hence $\wp(z)$ is of order 2.

As a consequence of well-known Jensen's formula, we get that the number of zeros of an entire function of order $\leq \rho$, inside a circle of radius R is at most $O(R^\rho)$ as $R \to \infty$. We will use these facts to show the algebraic independence of certain classical functions below. It is well known that e^z is a transcendental function. We show the following result.

Lemma 1.1.1 *For any non-zero $a \in \mathbb{C}$, the functions z and e^{az} are algebraically independent over $\mathbb{C}$.*

Proof Suppose the lemma is false. Then there exists a non-zero polynomial $P(x_1, x_2)$ such that $P(e^{az}, z) = 0$ for all $z \in \mathbb{C}$. We shall take the polynomial P to be of least degree in x_1. Let the degree of P in x_1 be ν. Thus there exist non-zero polynomials $f_0(z), \ldots, f_\nu(z) \in \mathbb{C}[z]$, not all constants such that $f_0(z) \not\equiv 0$ and

$$f_0(z)e^{\nu az} + f_1(z)e^{(\nu-1)az} + \cdots + f_\nu(z) = 0.$$

Divide out by $f_0(z)$ to get an equation of the form

$$Q(z) = e^{\nu az} + g_1(z)e^{(\nu-1)az} + \cdots + g_\nu(z) = 0$$

with $g_i(z) = f_i(z)/f_0(z)$ for $1 \leq i \leq \nu$. Note that $Q(z)$ is uniquely determined since ν is the least degree in x_1. We know that e^{az} is invariant under $z \to z + 2n\pi i/a, n \in \mathbb{Z}$. Thus each $g_i(z), 1 \leq i \leq \nu$ must be invariant under these transformations. That is, $g_i(z) = g_i(z + 2n\pi i/a)$. That means each $g_i(z)$ has either infinitely many zeros or poles. Since g_i is a rational function, we conclude each $g_i(z)$ is a constant which is a contradiction. □

By similar argument, we can also show the following lemma.

Lemma 1.1.2 *The functions e^z and e^{az}, a irrational are algebraically independent over $\mathbb{C}$.*

Proof Suppose the lemma is false. Arguing as in Lemma 1.1.1, there exists a unique relation

$$Q(z) = e^{\nu az} + g_1(e^z)e^{(\nu-1)az} + \cdots + g_\nu(e^z) = 0$$

with $g_i(e^z) = f_i(e^z)/f_0(e^z)$ for $1 \le i \le \nu$. Again, each $g_i(e^z)$ must be invariant under the transformation $z \to z + 2n\pi i/a$, $n \in \mathbb{Z}$. Since a is irrational, each $g_i(e^z)$ has two independent periods $w_1 := 2\pi i$ and $w_2 := 2\pi i/a$ and so $\ell_1 w_1 + \ell_2 w_2$ is a period for any integers ℓ_1 and ℓ_2. Hence, the number of zeros or poles inside a circle of radius R of any $g_i(e^z)$ is bounded below by $O(R^2)$. This is a contradiction as the order of $g_i(e^z)$ is 1. □

Another important function which has been widely studied is the Weierstrass elliptic function $\wp(z)$. This is a doubly periodic meromorphic function which is a quotient of entire functions of order 2. In fact, these entire functions are known as σ functions. For various properties of this function which will be used in this book, we refer to [1].

Lemma 1.1.3 *Let $\wp(z)$ and $\wp^*(z)$ be two elliptic functions with periods (ω_1, ω_2) and (ω_1^*, ω_2^*). Then $\wp$ and $\wp^*$ are algebraically dependent if and only if their periods are commensurable i.e there exists a 2×2 rational matrix M such that*

$$\begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} = M \begin{pmatrix} \omega_1^* \\ \omega_2^* \end{pmatrix}. \tag{1.1}$$

Proof Suppose there exists $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ satisfying (1.1) with $a, b, c, d \in \mathbb{Q}$. Then

$$\omega_1 = a\omega_1^* + b\omega_2^*;\ \omega_2 = c\omega_1^* + d\omega_2^*.$$

Hence there exists an integer m such that

$$m\omega_1 = a'\omega_1^* + b'\omega_2^*;\ m\omega_2 = c'\omega_1^* + d'\omega_2^*$$

with $a', b', c', d' \in \mathbb{Z}$. (One may take m to be the least common multiple of the denominators of a, b, c, d). Thus $\wp^*(mz)$ has fundamental periods ω_1 and ω_2. Hence $\wp^*(mz)$ is a rational function of $\wp(z)$. A priori, $\wp^*(mz)$ is a rational function of $\wp^*(z)$ which therefore implies that $\wp(z)$ and $\wp^*(z)$ are algebraically dependent.

Now we prove the converse. Suppose $\wp(z)$ and $\wp^*(z)$ are algebraically dependent. Arguing as in Lemma 1.1.1 there exists a unique relation

$$Q(z) = \wp(z)^\nu + g_1(\wp^*(z))\wp(z)^{(\nu-1)} + \cdots + g_\nu(\wp^*(z)) = 0$$

with $g_i(\wp^*(z)) = f_i(\wp^*(z))/f_0(\wp^*(z))$ for $1 \le i \le \nu$. Then each $g_i(\wp^*(z))$ is invariant under $z \to z + m\omega_1$, $m \in \{0, 1, 2, \ldots\}$ and under $z \to z + n\omega_2$, $n \in \{0, 1, 2, \ldots\}$. This means $\wp^*(z + m\omega_1)$ and $\wp^*(z + n\omega_2)$ are not all distinct. Hence there exist integers m_0 and n_0 such that $m_0\omega_1$ and $n_0\omega_2$ are periods of $\wp^*(z)$. Thus for some integers m_1, m_2, n_1, n_2 we have $m_0\omega_1 = m_1\omega_1^* + m_2\omega_2^*$ and $n_0\omega_1 = n_1\omega_1^* + n_2\omega_2^*$ which proves (1.1). □

1.2 Gauss's Lemma

Let $P(z) \in \mathbb{Z}[z]$ be a polynomial. Let $C(P)$ denote the greatest common divisor of the coefficients of P, and it is called the *content* of P. We say $P(z)$ is a *primitive polynomial* if $C(P) = 1$. We show

Lemma 1.2.1 *The product of two primitive polynomials is a primitive polynomial. Thus for any two polynomials $P, Q \in \mathbb{Z}[z]$ we have $C(PQ) = C(P)C(Q)$.*

Proof Let $P(z)$ and $Q(z)$ be two primitive polynomials with coefficients in $\mathbb{Z}$. Suppose their product PQ is not primitive. Then there exists a prime p such that

$$P(z)Q(z) \text{ is identically zero in } \mathbb{Z}/p\mathbb{Z}[z],$$

which we write as $P(z)Q(z) \equiv 0 \pmod{p}$. Let $P_1(z)$ and $Q_1(z)$ be the polynomials $P(z)$ and $Q(z)$ reduced $\pmod{p}$., i.e. $P_1(z) \equiv P(z) \pmod{p}$ and $Q_1(z) \equiv Q(z) \pmod{p}$. Hence

$$P_1(z)Q_1(z) \equiv 0 \pmod{p}. \tag{1.2}$$

Since $P(z)$ and $Q(z)$ are both primitive, $P_1(z)$ and $Q_1(z)$ are not identically 0. Let p_1 and q_1 be the leading coefficients of P_1 and Q_1, respectively. Then $p_1 \not\equiv 0 \pmod{p}$, $q_1 \not\equiv 0 \pmod{p}$ and hence $p_1 q_1 \not\equiv 0 \pmod{p}$. This contradicts (1.2). Thus PQ is primitive.

Any polynomial $P(z) \in \mathbb{Z}[z]$ can be written as $P(z) = C(P)P'(z)$ with P' primitive. If $R = PQ$, then $C(R)R' = C(P)C(Q)P'Q'$. Since $P'Q'$ is primitive, it follows that $C(R) = C(P)C(Q)$. □

It is possible to generalise the above result to any number of variables as follows.

Lemma 1.2.2 *Let $P, Q \in \mathbb{Z}[z_1, \ldots, z_m]$. Then*

$$C(PQ) = C(P)C(Q).$$

For a proof, we refer to Cassels [2]. It follows from the above lemmas that if P can be factored over $\mathbb{Q}$, it can also be factored over $\mathbb{Z}$.

Lemma 1.2.3 *Let $1 \le r < m$. Suppose that $F(z_1, \ldots, z_m) \in \mathbb{Z}[z_1, \ldots, z_m]$, $G(z_1, \ldots, z_r) \in \mathbb{Q}[z_1, \ldots, z_r]$ and $H(z_{r+1}, \ldots, z_m) \in \mathbb{Q}[z_{r+1}, \ldots, z_m]$ such that*

$$F(z_1, \ldots, z_m) = G(z_1, \ldots, z_r)H(z_{r+1}, \ldots, z_m).$$

Let γ be a coefficient in F. Then there is a factorisation $\gamma = \alpha\beta$ in $\mathbb{Q}$ such that $\alpha G \in \mathbb{Z}[z_1, \ldots, z_r]$ and $\beta H \in \mathbb{Z}[z_{r+1}, \ldots, z_m]$.

Proof Let the coefficients of G be $\alpha_1, \ldots, \alpha_s$ and that of H be $\beta_1, \ldots, \beta_t$ in some order. Since the variables in G and H are disjoint, the coefficients of F are $\alpha_i\beta_j$ and they are all in $\mathbb{Z}$. In particular, $\alpha_1\beta_j \in \mathbb{Z}$ for $1 \le j \le t$ and $\beta_1\alpha_j \in \mathbb{Z}$ for $1 \le j \le s$.