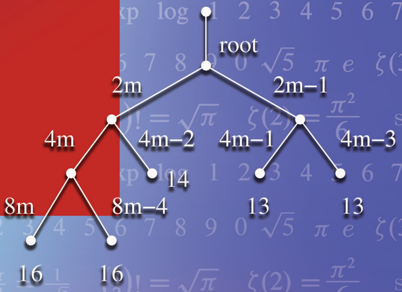
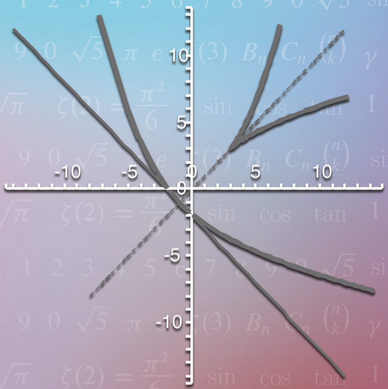
STUDENT MATHEMATICAL LIBRARY
Volume 65

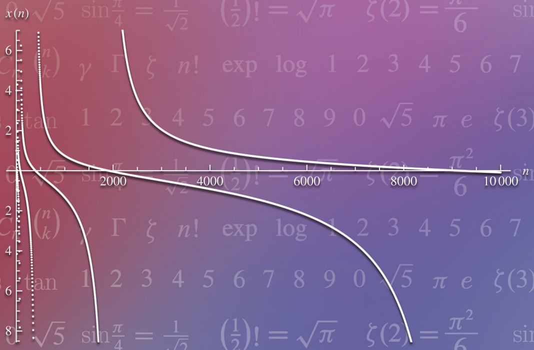
Numbers and Functions

From a classical-experimental mathematician's point of view

Victor H. Moll







AMS
American Mathematical Society

Numbers and Functions

From a classical-experimental mathematician's point of view

STUDENT MATHEMATICAL LIBRARY
Volume 65

Numbers and Functions

From a classical-experimental mathematician's point of view

Victor H. Moll

AMS
American Mathematical Society
Providence, Rhode Island

Editorial Board

Satyan L. Devadoss
Gerald B. Folland (Chair)
John Stillwell
Serge Tabachnikov

2010 *Mathematics Subject Classification.* Primary 05A05, 05C05, 11A07, 11A41, 11A55, 11B39, 11B65, 33B10, 33B15, 33F10.

For additional information and updates on this book, visit
www.ams.org/bookpages/stml-65

Library of Congress Cataloging-in-Publication Data

Moll, Victor H., 1956–
Numbers and functions : from a classical-experimental mathematician's point of view / Victor H. Moll.
p. cm.
Includes bibliographical references and index.
ISBN 978-0-8218-8795-0 (alk. paper)
1. Functions—Textbooks. 2. Calculus—Textbooks. I. Title.

QA331.M72 2012
515′.25–dc23

2012014772

Copying and reprinting. Individual readers of this publication, and nonprofit libraries acting for them, are permitted to make fair use of the material, such as to copy a chapter for use in teaching or research. Permission is granted to quote brief passages from this publication in reviews, provided the customary acknowledgment of the source is given.

Republication, systematic copying, or multiple reproduction of any material in this publication is permitted only under license from the American Mathematical Society. Requests for such permission should be addressed to the Acquisitions Department, American Mathematical Society, 201 Charles Street, Providence, Rhode Island 02904-2294 USA. Requests can also be made by e-mail to reprint-permission@ams.org.

© 2012 by the author. All rights reserved.
Printed in the United States of America.

∞ The paper used in this book is acid-free and falls within the guidelines
established to ensure permanence and durability.
Visit the AMS home page at http://www.ams.org/

10 9 8 7 6 5 4 3 2 1   17 16 15 14 13 12

Dedicated to Olivier Espinosa

Contents

Preface

In the process of writing a mathematics book, an author has to make a variety of decisions. The central theme of the book must be followed by deciding on a potential audience to whom the book is directed, and then a choice of style for presenting the material must be made.

This book began as a collection of additional notes given to students participating in the courses taught by the author at Tulane University. These courses included:

• **The calculus sequence**. This is the typical two-semester course on differential and integral calculus. The standard book used at Tulane is J. Stewart [**281**]. The author has used M. Spivak [**277**] for the Honor section, which is slightly more advanced than the regular one.

• **Discrete mathematics**. This course introduces students to mathematical induction and provides a glimpse of number theory. This is the first time where the students are exposed to proofs. The books used in the past include M. Aigner [**4**] and K. Rosen [**256**].

• **Combinatorics**. This is a one-semester course that includes basic counting techniques, recurrences, combinatorial identities, and the ideas behind bijective proofs. The author has used a selection of texts, including T. Andreescu and Z. Feng [**17**], A. Benjamin and J. Quinn [**46**], M. Bona [**58**], and R. Brualdi [**82**].

• **Number theory**. This is also a one-semester course covering the basics of the subject: primality and factorization, congruences, diophantine equations, continued fractions, primitive roots, and quadratic reciprocity. The texts used by the author include G. H. Hardy and E. M. Wright [**160**], K. Ireland and M. Rosen [**178**], K. Rosen [**257**], and J. H. Silverman [**274**].

• **Real analysis**. This is one of the few required courses for a mathematics major. It introduces the student to the real line and all of its properties. Sequences and completeness, the study of the real line, continuity, and compactness form the bulk of the course. The author has employed O. Hijab [**168**] and E. Landau [**192**] to reflect his opinion that this class should be calculus "well done".

• **Experimental mathematics**. This is a course created by the author. Notwithstanding that it has been taught only three times to date, it has been received very well by our students. The material in the course includes an introduction by the author to the symbolic language `Mathematica` and to `Maple` by a second instructor. The topics have included an introduction to computer proofs in the Wilf-Zeilberger style, recurrences, symbolic integration, and graph theory. Beyond using the computer as a number cruncher, the course has employed symbolic packages to discover new mathematical patterns and relationships, to create impressive graphics to expose mathematical structure, and to suggest approaches to formal proofs. The author has used the texts by J. M. Borwein and D. H. Bailey [**69**] and the second volume written jointly with R. Girgensohn [**70**] as well as the lecture notes [**36**] from a course in experimental mathematics given by the authors at the Joint Mathematics Meetings in San Antonio. The volume by M. Petkovsek, H. Wilf, and D. Zeilberger [**247**] has been used to lecture on automatic proofs. The audience for this class has consisted of students majoring in mathematics and some others who wandered into the class because they heard that the topics were interesting.

The author has always placed a special effort in his lectures to point out that material covered in a specific class is part of a bigger picture. This book is a product of notes written for these courses.

Naturally, most of the topics covered appear in the literature. It is the point of view that is new.

The present book contains a variety of topics that at first reading might appear to be disconnected. It is the author's hope that in the end it will all fit together. The author finds some results in elementary mathematics particularly appealing and some material has been written to supply background towards a specific goal. No effort has been made to be systematic and there is no claim about the topics that do not appear here.

The reader will find here examples that include the following:

Evaluation of finite sums. These are used as examples to practice induction, to provide combinatorial interpretations, and to introduce the reader to ideas behind **automatic proofs**. The questions dealing with the evaluation of

$$\sum_{k=0}^{n} \binom{n}{k}^2 = \binom{2n}{n}$$

and the analogous problem for

$$\sum_{k=0}^{n} \binom{n}{k}^3$$

are in the background.

Prime factorization. The fundamental theorem of arithmetic states that every natural number has a unique decomposition as a product of primes. There are some beautiful results that describe this prime factorization for interesting sequences. These are expressed in terms of the so-called valuation $\nu_p(m)$, the highest power of the prime p that divides m. Among them is Legendre's formula for **factorials**, usually given as a series

$$\nu_p(n!) = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor,$$

but it can also be reinterpreted as

$$\nu_p(n!) = \frac{n - s_p(n)}{p-1}.$$

Here $s_p(n)$ is the sum of digits of n written in base p.

The book explores properties of these prime factorizations for many classical sequences that come from combinatorics. These include **binomial coefficients**, which are encountered in the most elementary counting problems; **Catalan numbers**, which count the number of ways to place parentheses to group symbols in a sequence of numbers; the **Fibonacci numbers**, which count the ways to cover a board with squares and dominoes; the **Stirling numbers**, which count the number of ways to split a set of n elements into k nonempty parts; and many others. The patterns of the valuations of these sequences are sometimes remarkably beautiful and, in many cases, still need to be explained. Some of these families of numbers are unexpectedly related. For instance, computing the residues of the binomial coefficient $\binom{2p-1}{p-1}$ modulo powers of the prime p, the reader will encounter the **harmonic numbers** $H_n = 1 + \frac{1}{2} + \cdots + \frac{1}{n}$ and the **Bernoulli numbers** defined by the expansion of $x/(e^x - 1)$.

Elementary functions. The student finds a variety of functions in the beginning sequence of calculus. This book contains a study of polynomials, rational functions, exponentials/logarithms, and trigonometric functions. The author has made an effort to illustrate properties of these functions that hopefully the reader will find appealing. A variety of examples of polynomials appear in the book. These include **Bernoulli polynomials**, which provide the evaluation of well-known examples such as

$$\sum_{k=1}^{n} k^2 = \frac{n}{6} + \frac{n^2}{2} + \frac{n^3}{3}$$

and the less well known

$$\sum_{k=1}^{n} k^8 = \frac{n^9}{9} + \frac{n^8}{2} + \frac{2n^7}{3} - \frac{7n^5}{15} + \frac{2n^3}{9} - \frac{n}{30}.$$

It is easy to see that the sum of ath powers from 1 to n is a polynomial in n of degree $a+1$. The properties of the coefficients are a different story. These coefficients, the so-called **Bernoulli numbers**, are always rational numbers and their denominators can be described in relatively simple terms. It is a remarkable fact, one that the author always enjoyed, that the numerators are related to Fermat's last theorem, now established by A. Wiles, namely that the equation $x^n + y^n = z^n$ has no solutions in nonzero integers when $n \geq 3$.

Roots of polynomials are encountered by the student in the courses preparing him or her for the calculus sequence. This book treats the cases of degree 3 and 4 by expressing the roots by radicals and then in terms of one trigonometric function. In future courses the student will most likely learn that, in general, **there is no expression by radicals for the solution of a quintic equation**. This celebrated result of Abel and Galois is one of the jewels of the nineteenth century and it must be studied. On the other hand, it is possible to express the roots of any polynomial equation in terms of more advanced functions. Elliptic functions suffice for degree 5 or 6 and the so-called theta functions produce solutions for higher degrees. This is a beautiful subject that also deserves to be studied. From this point of view, the best way to solve a cubic equation is via trigonometric functions. This is an overstatement: the student should be aware of both methods.

Rational functions are introduced as coming from **generating functions** of sequences that obey linear recurrences with constant coefficients. The main example is that of the Fibonacci numbers, defined by $F_n = F_{n-1}+F_{n-2}$, with initial conditions $F_0 = 0$ and $F_1 = 1$. Their generating function is

$$\sum_{n=0}^{\infty} F_n x^n = \frac{x}{1-x-x^2}.$$

The classical question of how to integrate a rational function is probably the first time that a student seriously deals with this class. The method of partial fractions, which provides the solution to this question, is discussed in detail. One of the earliest evaluations of an integral in closed form, the **Wallis formula**

$$\int_0^\infty \frac{dx}{(x^2+1)^{m+1}} = \frac{\pi}{2^{2m+1}}\binom{2m}{m}$$

is established by a variety of methods.

This book contains two examples of transformations on the class of rational functions. The first example is

$$R(x) \mapsto \frac{R(\sqrt{x}) - R(-\sqrt{x})}{2\sqrt{x}}$$

and it originated from an attempt by the author to develop a new method of integration. The map above comes from separating the integrand R into its even and odd parts. Iterating this transformation to a function of the type $x^j/(x^m-1)$ has unexpected number theoretical properties. The second type of transformation comes from the rational function $R(x) = \dfrac{x^2-1}{2x}$, coming from the relation between $\cot\theta$ and $\cot 2\theta$. Using this rational function as a change of variable, one finds remarkable identities among integrals. These are the so-called ***Landen transformations***, which produce identities of the type

$$\int_{-\infty}^{\infty} \frac{dx}{ax^2+bx+c} = \int_{-\infty}^{\infty} \frac{dx}{a_1x^2+b_1x+c_1}$$

where

$$a_1 = \frac{2ac}{c+a}, \quad b_1 = \frac{b(c-a)}{c+a}, \quad c_1 = \frac{(c+a)^2-b^2}{2(c+a)}.$$

It turns out that iterating this procedure gives a sequence (a_n, b_n, c_n) and a number L such that $a_n \to L$, $b_n \to 0$, and $c_n \to L$. The invariance of the integral leads to the identity

$$\int_{-\infty}^{\infty} \frac{dx}{ax^2+bx+c} = \frac{\pi}{L}.$$

This shows that the integral may be computed numerically by computing the sequence $\{a_n\}$. These types of ideas extend to the computation of **the integral of any rational function on** $\mathbb{R}$. Details appear in Chapter 15.

Transcendental functions appearing in the book include some of elementary type such as **exponential**, **trigonometric**, and **hyperbolic** functions. These complete the class of elementary functions treated in the calculus sequence. The goal is to provide interesting properties of these functions and to describe connections with combinatorics, number theory, and interesting numbers. For instance, the reader will see that the expansion of some trigonometric functions around the origin involves the Bernoulli numbers mentioned in the context of evaluation of power sums.

The basic constants of analysis, e and π, are discussed in detail. Their irrationality is established by a systematic method. It is intriguing that the irrationality of $e+\pi$ is still an open problem. Their **continued fractions**, which provide optimal approximations by rational numbers, are established. There are some beautiful integral evaluations related to this topic. An example is given by

$$\int_0^1 \frac{x^4(1-x)^4}{1+x^2}\,dx = \frac{22}{7} - \pi,$$

which proves that $\pi \neq \frac{22}{7}$. There is a marked difference in the behavior of these continued fractions. The patterns for e are quite regular, while those for π remain a mystery. The appearance of e in a combinatorial setting is given by the counting of permutations of n objects that do not fix a single one of them. This is the classical **derangement number**. Its behavior for large n is related to e. This is totally unexpected.

The author has chosen two examples of nonelementary transcendental functions to illustrate some of their properties. The first one is the **gamma function** $\Gamma(x)$ (and its logarithmic derivative: the **digamma function** $\psi(x) = \Gamma'(x)/\Gamma(x)$) introduced by Euler, and the second one is the **Riemann zeta function** $\zeta(s)$ coming from questions dealing with the distribution of prime numbers.

Irrationality questions are considered throughout the book. The irrationality of some special numbers is presented in detail. These include $\sqrt{2}$, e, π, and also $\zeta(2) = \pi^2/6$ and $\zeta(3)$. This last constant does not admit a simpler representation. Its irrationality, recently established by R. Apéry, is discussed in the last chapter. It is unknown whether it is a rational multiple of π^3. The arithmetic properties of the **Euler constant**, defined by $\gamma = -\Gamma'(1)$, are still unknown. Some details on this question are described.

Symbolic computations are seen as an essential ingredient of this book. `Mathematica` examples are included to illustrate the capabilities of this language. In an earlier draft of the book there was a separate chapter describing the methods developed by Sister Celine and by W. Gosper Jr. and the WZ-theory created by H. Wilf and D. Zeilberger. The final draft incorporates these techniques into the flow of the book.

This book started as a collection of notes written for a variety of courses. The author has tried to give credit to the authors of the various notes. It is very likely that some of them have been missed. **My apologies to those ignored or misquoted**. There are many books that have been used to obtain the information presented here. These are the author's favorite ones, starting with the classic **Modern Analysis** by E. T. Whittaker and G. N. Watson [**311**]; the basic treatment on automatic proofs can be found in the text by M. Petkovsek, H. Wilf, and D. Zeilberger [**247**]; and the book by R. Graham, D. Knuth, and O. Patashnik [**145**] is a great source for a class in discrete mathematics. The best introduction to the issues of symbolic computation is given in the text by M. Kauers and P. Paule [**181**]. From there the reader should consult the information provided on the website

`http://www.risc.jku.at/`

from RISC (the Research Institute for Symbolic Computation) at the Johannes Kepler University in Linz, Austria, and

`http://carma.newcastle.edu.au`

from the Priority Research Centre for Computer-Assisted Research Mathematics and Its Applications (CARMA) at the University of Newcastle, Australia. The order in which these two centers were listed does not imply a preference by the author.

Experimental mathematics is a relatively new name for an old approach to doing mathematics. It seems optimal to quote the gurus of the field about their opinions on what experimental mathematics is.

In [**143**], H. Wilf describes the path from experiment to theory in mathematics as follows: *"... it begins with wondering what a par-*

ticular situation looks like in detail; it continues with some computer experiments to show the structure of that situation for a selection of small values of the parameters of the problem; and then comes the human part: the mathematician gazes at the computer output, attempting to see and to codify some patterns. If this seems fruitful, then the final step requires the mathematician to prove that the apparent pattern is really there, and it is not a shimmering mirage above the desert sands."

D. Zeilberger in [**322**] and in many of his other articles and opinions proposes to *eliminate the human factor* in the mathematical experience. Perhaps *eliminate* is too strong of a word and *minimize* is more pleasant. But Doron does not mince words, so neither does the author. The reality is that more and more mathematics is becoming part of the computer experience. The author remembers spending hours of valuable high school time extrapolating tables of logarithms. Then came the hand calculator....

J. M. Borwein and D. H. Bailey [**69**] enumerate the role of computing in mathematics: (i) gaining insight and *intuition*; (ii) *discovering* new relationships; (iii) *visualizing* mathematical principles; (iv) *testing* and especially *falsifying* conjectures; (v) *exploring* a possible result to see if it *merits* formal proof; (vi) *suggesting* approaches for formal proof; (vii) *computing* replacing lengthy hand derivations; (viii) *confirming* analytically derived results. A nice collection of examples illustrating this point of view of mathematics is provided in [**34, 35**].

The author has tried to follow this list in the context of undergraduate material. Aside from that, he has aimed to present elementary results from a novel point of view, hoping to motivate the reader to learn more about standard subjects. It is clear that some statements have shorter proofs than the one presented in the text. The students have always been in the background of the writing, so sometimes it is instructive to present a complicated proof: the point illustrated is that often that is all you can do. This is fine. If you find a nicer argument later, even better.

Most of the topics are from **elementary mathematics** with occasional hints on how it connects to more sophisticated subjects. Part of the motivation for bringing together a large collection of notes on diverse topics was to provide the reader with some fun while learning interesting pieces of mathematics. *It was a lot of fun to write the book. Hopefully the reader will enjoy part of it.*

The final version of this book has been improved by many comments received by colleagues, students, and friends. A partial list is

Tewodros Amdeberhan	Tulane University
Valerio De Angelis	Xavier University, New Orleans
Erin Beyerstedt	Tulane University
Jon Borwein	CARMA, University of Newcastle, Australia
Peter Bull	Tulane University
Michael Hirschhorn	University of New South Wales, Sydney, Australia
Manuel Kauers	RISC Institute, Linz, Austria
Karen Kohl	Tulane University
Christoph Koutschan	RISC Institute, Linz, Austria
Dante Manna	Wesleyan University, Virginia
Luis A. Medina	Universidad de Puerto Rico, Rio Piedras
Tom Osler	Rowan University, New Jersey
Eric Rowland	Tulane University
Armin Straub	Tulane University
Jonathan Sondow	New York City
Xinyu Sun	Xavier University, New Orleans
Wadim Zudilin	CARMA, University of Newcastle, Australia

The author especially wishes to recognize the contribution of

Allen Stenger Alamogordo, New Mexico,

who provided detailed comments in each chapter of this manuscript.

Special thanks to the staff at the Department of Mathematics at Tulane University for their help during the time when this book was being prepared. In particular, many thanks to Augusta (Cammy) Watts for her help finding every possible paper that had a relation to the topics covered here.

This book was completed in the fall of 2011 and the author wishes to acknowledge the hospitality provided by the Courant Institute of New York University during this period.

The author was supported in part by NSF Grant #0713836. Finally, the author wishes to thank the staff of the AMS and especially Ed Dunne. His periodic emails were part of the motivation to convert a large collection of notes into the current book.

Chapter 1

The Number Systems

The goal of this chapter is to introduce the different kinds of numbers that will appear throughout the text. We start with an intuitive treatment of the **natural numbers** $\mathbb{N}$. This is followed by a description of the **integers** $\mathbb{Z}$ and **rational numbers** $\mathbb{Q}$. The question of completion of rational numbers leads to **real numbers** $\mathbb{R}$ and to the set of ***p*-adic numbers** $\mathbb{Q}_p$, one set per prime number p. These are all the completions of $\mathbb{Q}$. The chain of number systems culminates with **complex numbers** $\mathbb{C}$. The text by H. Ebbinhaus et al. [**120**] gives a description of the number systems presented here, with many of the historical facts associated to them.

1.1. The natural numbers

This section contains a very intuitive approach to the set of **natural numbers**

$$\mathbb{N} := \{1, 2, 3, \ldots\} \tag{1.1.1}$$

as is encountered in childhood. These are the **counting numbers**. The reader will find in the text by Y. Moschovakis [**225**] a more axiomatic development of this set.

The **successor function** is one of the fundamental concepts in the definition of the set $\mathbb{N}$. The successor of $n \in \mathbb{N}$ is denoted by n^+.

Part of the axiomatic development of $\mathbb{N}$ is to impose some properties on this function:

- The map $n \mapsto n^+$ is one-to-one; that is, if $n_1^+ = n_2^+$, then $n_1 = n_2$.
- The number 1 is not the successor of any natural number.
- If $M \subset \mathbb{N}$ contains 1 and is closed under successor (that is, if $n \in M$, then $n^+ \in M$), then $M = \mathbb{N}$.

The last property is the familiar **principle of mathematical induction**.

Exercise 1.1.1. Prove that $\mathbb{N} = \{1\} \cup \{n^+ : n \in \mathbb{N}\}$.

Note 1.1.2. The fact that the function $n \mapsto n^+$ is one-to-one and the previous exercise imply that for every $m \in \mathbb{N}$, $m \neq 1$, there is a unique natural number, denoted by m_-, such that $m_-^+ = m$. The number m_- is called the **predecessor** of m.

Note 1.1.3. The usual notation for natural numbers can be given a more rigorous approach by *defining*

$$1^+ = 2, \tag{1.1.2}$$

and then,

$$2^+ = 3, \tag{1.1.3}$$

that is, $3 = (1^+)^+$. The principle of induction states that $\mathbb{N}$ consists of all the images of the number 1 under the successor function.

Note 1.1.4. E. Landau [**192**] defines the numbers 2, 3, ..., 9 in terms of the successor function and then proceeds to prove all elementary properties of arithmetic in terms of the decimal expansions of natural numbers. The point of view taken here is less rigorous. The elementary arithmetical properties of natural numbers are taken for granted. The operation of **addition** can be defined using the successor function in the following form: fix $m \in \mathbb{N}$ and define $m + n$ by

$$\begin{aligned} m+1 &= m^+ \text{ (the successor of } m\text{)}, \\ m+n &= (m+n_-)^+ \quad \text{for } n \neq 1. \end{aligned}$$

Here n_- is the predecessor of n. A similar definition of multiplication is possible. All the elementary properties of addition and multiplication in $\mathbb{N}$ can now be proved.

Exercise 1.1.5. The usual properties of addition and multiplication of natural numbers can all be established by induction. The reader is invited to check that $a + b = b + a$ and $(ab)^n = a^n b^n$ hold for $a, b, n \in \mathbb{N}$.

Note 1.1.6. An example of the themes developed in this book is the evaluation of finite sums in terms of a given class of special functions. The general idea is described with the sums

$$S_a(n) := \sum_{k=1}^{n} k^a, \quad a \in \mathbb{N}. \tag{1.1.4}$$

Given a class of functions $\mathfrak{F}$, the question is whether one can obtain the value of $S_a(n)$ in terms of a **fixed function** $f_a \in \mathfrak{F}$ evaluated at n. For example, the elementary evaluation

$$S_1(n) = \frac{1}{2}n(n+1) \tag{1.1.5}$$

shows that $S_1(n)$ can be expressed in terms of the class of polynomials with rational coefficients. These elementary facts are described in Chapter 4.

Exercise 1.1.7. Prove (1.1.5) by induction. **Hint for an alternative proof:** Observe that $S_1(n)$ satisfies $S_1(n+1) = S_1(n) + n + 1$. Define

$$T_1(n) := \frac{2}{n(n+1)}S_1(n) - 1 \tag{1.1.6}$$

and check that $T_1(n+1) = nT_1(n)/(n+2)$. The value $T_1(1) = 0$ gives the result.

1.2. An automatic approach to finite sums

The question of a closed form for a finite sum is solved in a completely elementary manner if the sum **telescopes**. These are sums of the form

$$A_n = \sum_{k=1}^{n} (f_{k+1} - f_k). \tag{1.2.1}$$

Cancellation occurs in A_n and its value is

$$A_n = f_{n+1} - f_1. \tag{1.2.2}$$

Exercise 1.2.1. Check that the sum

$$A_n = \sum_{k=1}^{n} k\, k! \tag{1.2.3}$$

can be evaluated by telescoping. **Hint:** Write $k = (k+1) - 1$. This hint is really a **trick**. See Exercise 1.2.4 for a solution without it.

The question of how to determine if a sum is of this form was answered by R. W. Gosper Jr. in [**140**]. The **automatic procedure** developed there is illustrated with the evaluation of

$$S_1(n) := \sum_{k=1}^{n} k = \frac{1}{2} n(n+1). \tag{1.2.4}$$

The transformation of a sum

$$B_n = \sum_{k=1}^{n} t_k \tag{1.2.5}$$

to telescoping form is translated to the existence of a function s_k such that

$$s_{k+1} - s_k = t_k. \tag{1.2.6}$$

If such a function can be found, then

$$B_n = s_{n+1} - s_1. \tag{1.2.7}$$

Gosper treated the class of summands where

$$r_k := \frac{t_{k+1}}{t_k} \tag{1.2.8}$$

is a rational function. These summands are said to be of **hypergeometric type** or simply **hypergeometric**. The algorithm starts by replacing the unknown s_k by the rational function y_k defined by $s_k = y_k t_k$. Then (1.2.6) becomes

$$r_k y_{k+1} - y_k = 1. \tag{1.2.9}$$

The next step requires a technical point: a factorization of the rational function r_k in the form

$$r_k = \frac{a_k}{b_k}\frac{c_{k+1}}{c_k} \tag{1.2.10}$$

where a_k, b_k, c_k are polynomial sequences such that a_k and b_{k+h} are relatively prime. The reader will find in the text by M. Petkovsek, H. Wilf, and D. Zeilberger [**247**] a proof of the fact that such a factorization always exists. The additional assumptions that the pairs $\{a_k,\, c_k\}$ and $\{b_k,\, c_{k+1}\}$ are relatively prime polynomials guarantees uniqueness of the factorization. Efficient algorithms for finding this factorization are also described.

The final change of the unknown, given by

$$y_k = \frac{b_{k-1}}{c_k}x_k, \tag{1.2.11}$$

converts (1.2.9) to

$$a_k x_{k+1} - b_{k-1}x_k = c_k. \tag{1.2.12}$$

The remarkable result of Gosper is stated next. The reader will find a proof in [**247**].

Theorem 1.2.2. *Let a_k, b_k, c_k be as described above. If x_k is a rational function that solves* (1.2.12)*, then x_k is a polynomial function.*

To complete the algorithm, determine bounds for the polynomial function x_k and solve (1.2.12) by the ansatz with undetermined coefficients and by backwards substitute to obtain s_k.

Example 1.2.3. Gosper's algorithm is illustrated with the sum (1.2.4). In this case $t_k = k$, so

$$r_k = \frac{k+1}{k} \tag{1.2.13}$$

is already in the required factored form (1.2.10) with $a_k = b_k = 1$ and $c_k = k$. The final equation (1.2.12) takes the form

$$x_{k+1} - x_k = k. \tag{1.2.14}$$

This is the same equation as the original one. Gosper's result now guarantees that, if (1.2.6) has a solution of hypergeometric type, then (1.2.14) has a polynomial solution. The reader can check that there is no solution of degree 1 in k, so x_k must be of degree at least 2. The form $x_k = ak^2 + bk + c$ replaced in (1.2.14) provides the solution $x_k = \frac{1}{2}k^2 - \frac{1}{2}k$. Returning to the original problem, it gives

$$s_k = \tfrac{1}{2}k^2 - \tfrac{1}{2}k. \tag{1.2.15}$$

Therefore

$$\begin{aligned} S_1(n) &= \sum_{k=1}^{n} k \\ &= \sum_{k=1}^{n} (s_{k+1} - s_k) \\ &= s_{n+1} - s_1 \\ &= \frac{n(n+1)}{2}, \end{aligned}$$

as expected.

Exercise 1.2.4. Use this algorithm to evaluate the sum in Exercise 1.2.1. The hint is no longer required.

Note 1.2.5. Most symbolic languages have implemented Gosper's algorithm. The command `Sum`, employed in `Mathematica` to deal with sums of hypergeometric terms, makes use of it. This gives the evaluation of a large variety of sums. For example, the input

$$\texttt{Sum}[k^2, k] \tag{1.2.16}$$

(followed by the `Expand` command to visualize the answer in a better form) gives the output

$$\frac{k}{6} - \frac{k^2}{2} + \frac{k^3}{3}. \tag{1.2.17}$$

Denote the function in (1.2.17) by $F(k)$. Then the reader can verify that $F(k+1) - F(k) = k^2$ and it follows that

$$S_2(n) := \sum_{k=1}^{n} k^2 = F(n+1) - F(1) = \frac{1}{6}n(n+1)(2n+1). \tag{1.2.18}$$

Exercise 1.2.6. The reader who insists on proving by induction a formula produced by Gosper's algorithm can still use it to reduce the amount of work required. This idea is illustrated with the evaluation of $S_2(n)$. Let

$$G_2(n) = \frac{n(n+1)(2n+1)}{6}$$

be the answer obtained from Gosper's algorithm. Now define

$$T_2(n) = \frac{S_2(n)}{G_2(n)} - 1.$$

Check that the recurrence $S_2(n+1) = S_2(n) + (n+1)^2$ produces

$$T_2(n+1) = \frac{n(2n+1)}{(n+2)(2n+3)} T_2(n). \tag{1.2.19}$$

Now use $T_2(1) = 0$ to conclude that $T_2(n) \equiv 0$.

Exercise 1.2.7. Prove a formula for $S_3(n) = \sum_{k=1}^{n} k^3$ along the lines indicated in Exercise 1.2.6.

Note 1.2.8. `Mathematica` contains the knowledge of a very large class of functions, so the output might surprise the reader. For instance,

$$\texttt{Sum}[1/k,\ k] \tag{1.2.20}$$

produces the output

$$\texttt{PolyGamma}[0, k]. \tag{1.2.21}$$

The **polygamma function** is the logarithmic derivative of the **gamma function**, sometimes called the **digamma function**. An elementary introduction to these functions is given in Chapter 16. The `Mathematica` `Sum` function gives the **indefinite sum** and it usually contains a *constant of summation*. For instance, the value `PolyGamma`[0,3] gives $\frac{3}{2} - \texttt{EulerGamma}$. This constant is defined by

$$\gamma = \texttt{EulerGamma} = \lim_{n \to \infty} \sum_{k=1}^{n} \frac{1}{k} - \ln n. \tag{1.2.22}$$

Exercise 1.2.9. Use Gosper's algorithm to prove that the digamma function is not hypergeometric. **Hint:** Apply the algorithm to the summand $1/k$.

There are simple summands when even Mathematica is unable to produce an answer. For example, for the nonhypergeometric entry,

$$\texttt{Sum}[1/(k+\sqrt{k}),k]$$

is returned as

$$\sum_k \frac{1}{\sqrt{k}+k} \tag{1.2.23}$$

without any further simplification. The fact is that there is no closed form for this sum. On the other hand, Mathematica also fails to evaluate the sum

$$\sum_{k=0}^{n}(1-\sqrt{k}+k)\sqrt{k!}=(n+1)\sqrt{n!}\,.$$

The reader will find in the book by M. E. Larsen [**195**] a description of the variety of methods developed to treat the question of evaluation of finite sums.

1.3. Elementary counting

A recurrent theme in this book is that certain numbers a_n are of interest because they appear as **counting sequences**. That is, there is a collection of sets A_n, indexed by $n \in \mathbb{N}$, such that

$$a_n = \text{ number of elements in } A_n. \tag{1.3.1}$$

As a first example, consider the number of subsets of

$$X_n := \{1,\, 2,\, \ldots,\, n\}; \tag{1.3.2}$$

that is,

$$A_n := \{Y : Y \subset X_n\}. \tag{1.3.3}$$

It is certain that the reader knows that $a_n = 2^n$.

Theorem 1.3.1. *The set X_n has 2^n subsets; that is, $a_n = 2^n$.*

Proof. Let a_n be the number of subsets of X_n. The proof consist in producing a recurrence for a_n that will be used to prove the result by induction. Concentrate on the last element $n+1$. The a_{n+1} subsets of X_{n+1} are divided into two disjoint classes: those that contain $n+1$

and those that do not. The sets of the second type can be put in a one-to-one correspondence with the subsets of X_n. Therefore, there are a_n sets of this type. On the other hand, any set of the first type is of the form $A \cup \{n+1\}$, with $A \subset X_n$. Therefore, $a_{n+1} = 2a_n$ and the result follows by induction. $\square$

Note 1.3.2. Given a recurrence, such as $a_{n+1} = 2a_n$ from which the first few values suggest a formula for a_n, it is often convenient to use the guessed expression to define a new variable. Then the recurrence for t_n is usually simpler than the original one. In the example considered here, let $t_n := 2^{-n}a_n$. Then t_n satisfies $t_{n+1} = t_n$. The initial value $t_1 = 1$ establishes that $t_n = 1$, proving that $s_n = 2^n$, for all $n \in \mathbb{N}$.

The second example of counting sequences deals with the concept of **permutations**. Start with a collection of objects

$$Y_n = \{y_1, \, y_2, \, \ldots, y_n\}. \tag{1.3.4}$$

In this context, a **bijection** $f : Y_n \to Y_n$ is called a **permutation** of the objects in Y_n. Recall that a bijection is a function that is one-to-one and onto. That is, for each index i in the range $1 \leq i \leq n$, there is a unique index j in the same range such that $f(y_i) = y_j$. The set of all permutations of Y_n is called the **symmetric group on** n **letters** and it is denoted by S_n. The question considered here is the number of elements in S_n. Denote this number by b_n. A formula for b_n will be obtained from a recursion.

In order to produce this recursion, the **multiplicative principle** of combinatorics is employed. The principle states that if the reader is asked to perform two consecutive experiments such that there are a_1 possible outcomes for the first task and for each of these the second task has a_2 possible outcomes, then the two events have a total of $a_1 \times a_2$ possible results. The goal is now to reduce a permutation on n symbols to one with fewer symbols. This is done using a standard way to represent a permutation via an array, with each column being of the form $\{y_i, f(y_i)\}$. For example, the array

$$\begin{pmatrix} y_1 & y_2 & y_3 & y_4 & y_5 & y_6 \\ y_3 & y_2 & y_6 & y_1 & y_4 & y_5 \end{pmatrix} \tag{1.3.5}$$

represent the function $f : \{y_1, \ldots, y_6\} \to \{y_1, \ldots, y_6\}$ such that $f(y_1) = y_3$, $f(y_2) = y_2$, and so on.

The reduction from n symbols to $n-1$ is described next. Let f be a permutation of Y_n. Choose an index i in the range $1 \leq i \leq n$ and assume $f(y_i) = y_j$. Drop y_i from the domain of f and drop y_j from its range. If $f(y_i) = y_i$, that is, if $i = j$, then the function f can be restricted to the set $\{y_1, y_2, \ldots, y_{i-1}, y_{i+1}, \ldots, y_n\}$ as a permutation. If $i \neq j$, then relabel the element y_i in the range as y_j. The function f restricted to the relabeled set is again a permutation. For example, suppose that f is given by (1.3.5). Then choose $i = 1$ and note that $f(y_1) = y_3$. Then the restricted function is obtained by dropping y_1 from the domain and y_3 from the range and finally relabeling y_3 as y_1 in the domain. This yields the modified function

$$\begin{pmatrix} y_2 & y_1 & y_4 & y_5 & y_6 \\ y_2 & y_6 & y_1 & y_4 & y_5 \end{pmatrix}. \tag{1.3.6}$$

There are n ways to choose y_i to start the construction and b_{n-1} ways to permute the new set. The multiplicative principle states that

$$b_n = n \times b_{n-1}. \tag{1.3.7}$$

Clearly $b_1 = 1$. The list of the first few values is $\{1, 2, 6, 24, 120\}$. This data suggests the formula

$$b_n = n! \tag{1.3.8}$$

where $n!$, the **factorial** of n, is the product of the first n natural numbers. This can be proved by induction using (1.3.7). Proceeding as in the previous example, define q_n by the relation $b_n = q_n \times n!$. The recurrence (1.3.7) yields $q_n = q_{n-1}$. The initial value $q_1 = 1$ gives $q_n = 1$ for all n. This proves the next statement.

Theorem 1.3.3. *There are $n!$ permutations of a set with n elements.*

Note 1.3.4. The values 1, 2, 6, 24, 120 listed above suggest (1.3.8) provided the reader has seen factorials before. (This is very likely to be the case.) A problem arises if the data generated produces a sequence not immediately recognized. For example, suppose the numbers

$$1,\ 2,\ 7,\ 42,\ 429,\ 7436 \tag{1.3.9}$$

appear in a calculation. Guessing the closed form

$$A_n = \prod_{j=0}^{n-1} \frac{(3j+1)!}{(n+j)!} \tag{1.3.10}$$

is now more difficult. Fortunately, there is a great database for sequences, created by N. Sloane, that will make suggestions to the reader. The site

`http://oeis.org/`

provides the reader with information about sequences. For instance, entering 1, 2, 6, 24 identifies them as the beginning of the factorial sequence. The site also provides information about where factorials appear in the literature. For instance, write the numbers from 1 to n on a circle. Then $n!$ counts the sum of the products of all $n-2$ adjacent numbers; for example,

$$5! = 1 \times 2 \times 3 + 2 \times 3 \times 4 + 3 \times 4 \times 5 + 4 \times 5 \times 1 + 5 \times 1 \times 2.$$

Sloane's database is an incredibly valuable tool. The numbers A_n count the so-called **alternating sign matrices**. This sequence appears as entry A005130 in the OEIS database. The reader will find some information about them in Chapter 7.

1.4. The integers and divisibility

The notion of order defined in $\mathbb{N}$ shows that, given $a,\ b \in \mathbb{N}$ with $a > b$, the equation $x + a = b$ has no solution in $\mathbb{N}$. The set of **integers** $\mathbb{Z}$ is defined in terms of these equations: to each pair $(a, b) \in \mathbb{N} \times \mathbb{N}$, the **integer** x is defined as the unique solution of $x + a = b$. It is denoted by $b - a$.

Exercise 1.4.1. Convince yourself that $\mathbb{Z}$ can be interpreted as pairs $(a, b) \in \mathbb{N} \times \mathbb{N}$ with the identification $(a, b) \sim (c, d)$ if and only if $a + d = b + c$.

Exercise 1.4.2. Prove that $\mathbb{N} \subset \mathbb{Z}$.

The next definition uses Exercise 1.4.1 to develop a more rigorous approach to $\mathbb{Z}$.

Definition 1.4.3. The set of integers $\mathbb{Z}$ is defined as the set of all equivalence classes. Let $[a, b]$ be the class of the pair (a, b); for example, $[2, 3] = -1$. The operations on $\mathbb{Z}$ are defined by

$$[a, b] + [c, d] := [a + c, b + d] \quad \text{and} \quad [a, b] \cdot [c, d] := [ac + bd, ad + bc].$$

There are many things to verify. This is due to the fact that the operation has been defined on a class **using a representative**. Whenever this is done, one needs to check that the result of the operation is **independent** of the choice of representative.

One of the fundamental topics discussed in this book deals with **divisibility properties** of integers.

Definition 1.4.4. Given a, $b \in \mathbb{N}$, if there is an integer q such that $a = bq$, then it is said that b **divides** a. The number b is called a **divisor** of a.

Definition 1.4.5. A positive integer $n > 1$ is called **prime** if its only divisors are 1 and n; otherwise, it is called **composite**. The number 1 is declared a **unit**; it is neither prime nor composite.

Prime numbers are discussed in Section 1.7. An elementary result is presented next.

Theorem 1.4.6. *Every natural number $n > 1$ has a prime divisor.*

Proof. Let $n \in \mathbb{N}$ and assume the result for every $m < n$. If n is prime, then n itself is the desired prime factor. Otherwise, n factors as $n = a \cdot b$. Induction shows that a and b have prime divisors and these divide n. □

1.5. The Euclidean algorithm

Some of the fundamental properties of $\mathbb{Z}$ are those related to divisibility questions. Consider the linear equation

$$ax + by = c \tag{1.5.1}$$

with integer coefficients a, b, c. The problem of solving the equation for x, $y \in \mathbb{Z}$ is used as a motivation for these ideas.

Let $P(x,y) = ax + by - c$. The rational solutions (x,y) are easy to obtain. For example, if $b \neq 0$, it follows that $y = -\frac{a}{b}x + \frac{c}{b}$ and each $x \in \mathbb{Q}$ produces a unique solution to (1.5.1). This shows that the set of rational solutions to (1.5.1) can be identified with $\mathbb{Q}$ itself. The situation is simpler if $b = 0$. In that case, $x = c/a$ is the only solution, provided $a \neq 0$.

Now consider the same equation, but look for integer solutions. An interesting phenomenon occurs. This is illustrated with an example: the equation

$$2x + 4y = 5 \tag{1.5.2}$$

has no integer solutions because the left-hand side is even and the right-hand side is odd.

Now let's go back to (1.5.1). Suppose there is an integer d such that d divides a and b and does not divide c. Then d divides the left-hand side of (1.5.1) but it does not divide the right-hand side. This contradiction shows that in this case there are no integral solutions. The largest such d is the **greatest common divisor** of a and b, denoted by $\gcd(a,b)$.

The complete analysis of equation (1.5.1) requires the **Euclidean algorithm**. Start with a basic result on division.

Exercise 1.5.1. Let a, $b \in \mathbb{Z}$. Prove the existence of integers q, r with $0 \leq r < b$ such that $a = bq + r$. Are these numbers unique? **Hint:** Fix b and prove the result by induction on a.

Now let $r_0 = a$ and $r_1 = b$. Exercise 1.5.1 produces

$$\begin{aligned} r_0 &= r_1q_1 + r_2, \quad 0 \leq r_2 < r_1, \\ r_1 &= r_2q_2 + r_3, \quad 0 \leq r_3 < r_2, \\ \cdots &= \cdots \\ r_{n-2} &= r_{n-1}q_{n-1} + r_n, \quad 0 \leq r_n < r_{n-1}, \\ r_{n-1} &= r_nq_n. \end{aligned} \tag{1.5.3}$$

Note that the sequence of remainders $r_0 > r_1 > \cdots > r_{n-1} > r_n$ is a strictly decreasing sequence of positive integers, so it has to stop after a finite number of steps. Let n be this number.

Exercise 1.5.2. Prove that r_n is the greatest common divisor of a and b.

Reading the steps of the Euclidean algorithm backwards, it follows that

$$r_n = r_{n-2} - r_{n-1}q_{n-1} \tag{1.5.4}$$

and then replacing

$$r_{n-1} = r_{n-3} - r_{n-2}q_{n-2} \tag{1.5.5}$$

yields

$$\begin{aligned} r_n &= r_{n-2} - q_{n-1}\left(r_{n-3} - r_{n-2}q_{n-2}\right) \\ &= \left(1 + q_{n-1}q_{n-2}\right) r_{n-2} - q_{n-1}r_{n-3}. \end{aligned}$$

Repeating this process shows the existence of u, $v \in \mathbb{Z}$ such that $r_n = au + bv$. This is called **an integer linear combination** of a and b.

Exercise 1.5.3. Prove that $d = \gcd(a, b)$ is the smallest positive integer that is an integer combination of a and b.

Definition 1.5.4. The integers a, b are called **relatively prime** if $\gcd(a, b) = 1$.

Exercise 1.5.5. Let a, $b \in \mathbb{N}$ and $d = \gcd(a, b)$. Prove that

$$\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1.$$

That is, a/d and b/d are relatively prime.

The analysis of (1.5.1) is presented next. To solve the equation (1.5.1), assume that d divides c and, actually dividing the equation by d, reduce it to

$$ax + by = c \quad \text{with } \gcd(a, b) = 1. \tag{1.5.6}$$

This can be solved using the Euclidean algorithm. First find integers u, v such that $au + bv = 1$. Now multiply by c to get that $x = uc$ and

$y = vc$ solve the equation. The next exercise is useful in determining the general solution of (1.5.6).

Exercise 1.5.6. Suppose a divides bc and $\gcd(a, b) = 1$. Prove that a divides c.

Theorem 1.5.7. *The equation $ax + by = c$ has no integer solutions x, y if $d = \gcd(a, b)$ does not divide c. In the other case, the general solution is given by*

$$x = x_0 - \frac{b}{d}t, \quad y = y_0 + \frac{a}{d}t,$$

where (x_0, y_0) is a particular solution and $t \in \mathbb{Z}$.

Exercise 1.5.8. Give all the details.

1.5.1. The length of the Euclidean algorithm.

The number of steps that it takes to compute the greatest common divisor of $a > b$ is estimated next. The **Fibonacci numbers**, defined by the recurrence

$$F_n = F_{n-1} + F_{n-2} \quad \text{with } F_1 = F_2 = 1, \tag{1.5.7}$$

make their first appearance. These numbers will be studied in Chapter 3.

Exercise 1.5.9. Let $\varphi = (1 + \sqrt{5})/2$ be the **golden ratio**. Prove that $F_n > \varphi^{n-2}$ for $n > 2$. The meaning of φ and its relation to Fibonacci numbers will become clear in Chapter 3.

Let q_i be the quotients obtained in the division of a by b. Observe that $q_1, q_2, \ldots, q_{n-1} \geq 1$ and $q_n \geq 2$. The first step is to prove $b \geq F_{n+1}$. This follows from $r_n \geq 1 = F_2$ and $r_{n-1} \geq 2r_n \geq 2F_2 = F_3$. Then

$$r_{n-2} \geq r_{n-1} + r_n \geq F_3 + F_2 = F_4.$$

Continuing in this form produces

$$r_2 \geq r_3 + r_4 \geq F_{n-1} + F_{n-2} = F_n,$$

and the next step yields $b \geq F_{n+1} > \varphi^{n-1}$. The approximation $\log_{10} \varphi \sim 0.208 > 1/5$ yields $\log_{10} b > (n-1)/5$. If $10^{k-1} \leq b < 10^k$, it follows that $n - 1 < 5k$ and therefore $n \leq 5k$. This proves a theorem of G. Lamé.

Theorem 1.5.10. *Let $a, b \in \mathbb{N}$ with $a > b$. The number of steps in the Euclidean algorithm is about* $\log_{10} n / \log_{10} \varphi$*. This is at most five times the number of decimal digits of* b*.*

Note 1.5.11. The average number of steps in the Euclidean algorithm to compute $\gcd(a, b)$, with $a \geq b$, has been shown to be approximately twice the number of digits of b.

Exercise 1.5.12. Prove that $\gcd(F_n, F_{n-1}) = 1$.

Exercise 1.5.13. Count the number of steps required to compute the greatest common divisor of F_{n+2} and F_{n+1}. Check that this gives the worst case scenario for Theorem 1.5.10.

1.5.2. The extended Euclidean algorithm. An economical way to implement the Euclidean algorithm using matrix row operations is discussed next. As a by-product of the procedure, $\gcd(a, b)$ is written as a linear combination of a and b without additional work. An example illustrates the general idea.

To compute $\gcd(144, 610)$, perform row operations on the augmented matrix of the trivial linear system

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 144 \\ 610 \end{pmatrix} \tag{1.5.8}$$

whose solution is $\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 144 \\ 610 \end{pmatrix}$. The first operation is to replace Row 2 with Row 2 $- \left\lfloor \frac{610}{144} \right\rfloor$Row 1 to produce

$$\left(\begin{array}{ccc} 1 & 0 & 144 \\ 0 & 1 & 610 \end{array} \right) \xrightarrow[R_2 - 4R_1]{} \left(\begin{array}{ccc} 1 & 0 & 144 \\ -4 & 1 & 34 \end{array} \right).$$

Next, replace Row 1 with Row 1 $- \left\lfloor \frac{144}{34} \right\rfloor$ Row 2:

$$\left(\begin{array}{ccc} 1 & 0 & 144 \\ -4 & 1 & 34 \end{array} \right) \xrightarrow[R_1 - 4R_2]{} \left(\begin{array}{ccc} 17 & -4 & 8 \\ -4 & 1 & 34 \end{array} \right).$$

Continue this way until one of the entries on the right is zero:

$$\begin{aligned}\begin{pmatrix} 17 & -4 & 8 \\ -4 & 1 & 34 \end{pmatrix} \quad \underset{R_2 - 4R_1}{\rightarrow} \quad & \begin{pmatrix} 17 & -4 & 8 \\ -72 & 17 & 2 \end{pmatrix} \\ \overset{R_1 - 4R_2}{\rightarrow} \quad & \begin{pmatrix} 305 & -72 & 0 \\ -72 & 17 & 2 \end{pmatrix}.\end{aligned}$$

The nonzero entry on the right gives the greatest common divisor $\gcd(144, 610) = 2$, and rewriting the corresponding linear system gives

$$-72\,(144) + 17\,(610) = 2.$$

Observe that the equation corresponding to the zero entry gives the least common multiple, $\operatorname{lcm}(144, 601)$. Indeed,

$$305 \times 144 - 72 \times 610 = 0$$

produces

$$305 \times 144 = 72 \times 610 = \operatorname{lcm}(144, 610).$$

Exercise 1.5.14. Prove that the above procedure works. **Sketch of the proof**: First convince yourself that one of the entries on the right *will* become zero. Then note that the row operations correspond to left multiplication by a matrix with integer entries and determinant 1. Now prove that if $Ax = v$, where all entries of A, x, v are integers, $\det A = 1$, and one of the entries of v is zero, then the other entry of v is the gcd of the entries of x, and the linear equation corresponding to the zero entry of v gives the least common multiple of the entries of x, as illustrated in the example.

1.5.3. The operation on integers.

The notion of **expansion with respect to a base** is introduced next. This will be used to describe an effective procedure to perform the basic operations on integers.

Theorem 1.5.15. *Given a, $b \in \mathbb{N}$, with $b > 1$, there exist nonnegative integers $x_0, x_1, \ldots, x_n$ such that*

$$a = x_0 + x_1 b + x_2 b^2 + \cdots + x_n b^n, \tag{1.5.9}$$

*with $0 \le x_i < b$ and $x_n \ne 0$. This is the **representation of** a **in base** b.*

Proof. The proof is by induction on a. The statement is clear for $a = 1$. Given a representation (1.5.9), if $x_0 < b - 1$, then

$$a + 1 = (x_0 + 1) + x_1 b + x_2 b^2 + \cdots + x_n b^n \tag{1.5.10}$$

is the desired representation of $a + 1$. In the case $x_0 = b - 1$, let j be the first index for which $x_j < b - 1$, if there is one. Thus

$$a = (b-1) + (b-1)b + (b-1)b^2 + \cdots + (b-1)b^{j-1} + x_j b^j + \cdots + x_n b^n,$$

and then,

$$\begin{aligned} a + 1 &= 1 + (b-1)(1 + b + b^2 + \cdots + b^{j-1}) + x_j b^j + \cdots + x_n b^n \\ &= b^j + x_j b^j + \cdots + x_n b^n \\ &= (1 + x_j) b^j + \cdots + x_n b^n \end{aligned}$$

is the desired representation. The final case is when all $x_j = b - 1$. Then

$$a = (b-1)(1 + b + \cdots + b^n) = b^{n+1} - 1$$

and therefore $a + 1 = b^{n+1}$. The proof is complete. □

Exercise 1.5.16. Prove that the representation of a in base b given above is unique.

Exercise 1.5.17. Implicit in the argument above is the familiar formula for the sum of a **geometric progression**: if $b \neq 1$, then

$$1 + b + b^2 + \cdots + b^n = \frac{b^{n+1} - 1}{b - 1}. \tag{1.5.11}$$

Prove it by induction.

The division algorithm can be used to obtain the representation of a in base b given in (1.5.9). The construction of the numbers x_i is achieved as follows: if $0 \leq a < b$, then $a = x_0$ is the representation. If not, divide a by b to obtain $a = bq + r$, with $0 \leq r < b$. Define $x_0 = r$. The next term in the sequence $\{x_i\}$ is obtained by dividing q by b. If $0 \leq q < b$, then define $x_1 = q$ and terminate. If not, write $q = bq_1 + r_1$ with $0 \leq r_1 < b$. Define $x_1 = r_1$ and produce $a = b^2 q_1 + b x_1 + x_0$. This process ends in a finite number of steps.

Exercise 1.5.18. Use the representation of integers in base b to discuss an efficient algorithm for adding natural numbers. The role of **carries** will appear in the context of binomial coefficients. See Theorem 2.6.7.

1.6. Modular arithmetic

One of the recurrent themes of the book is that of arithmetical properties of elementary functions. For instance, given a function defined by a power series

$$f(x) = \sum_{k=0}^{\infty} a_k x^k \tag{1.6.1}$$

with integer coefficients a_k, divisibility questions of these coefficients will be explored. The notion of **modular arithmetic** facilitates this discussion.

Let $n \in \mathbb{Z}$ be fixed and define a relation on $\mathbb{Z} \times \mathbb{Z}$ by

$$a \sim_n b \text{ if } b - a \text{ is divisible by } n. \tag{1.6.2}$$

This is an equivalence relation and the **integers modulo** n, denoted by $\mathbf{Z}_n$, is the space $\mathbb{Z} \times \mathbb{Z}$ where equivalent pairs are identified. The notation

$$a \equiv b \bmod n \tag{1.6.3}$$

is employed and $\mathbb{Z}_n$ is represented by

$$\mathbb{Z}_n := \{0,\, 1,\, 2, \ldots,\, n-1\}. \tag{1.6.4}$$

The arithmetical operations of addition and multiplication are defined as in $\mathbb{Z}$, now taking into account reduction modulo n. Division is slightly more complicated as not every element has an inverse in $\mathbb{Z}_n$. This is discussed in the next theorem.

Theorem 1.6.1. *Let $n \in \mathbb{N}$. Then $a \in \mathbb{Z}_n$ is invertible in $\mathbb{Z}_n$ if and only if* $\gcd(a, n) = 1$.

Proof. Assume $\gcd(a, n) = 1$. Then there are integers c, d such that $ac + nd = 1$. Therefore $ac \equiv 1 \bmod n$ and c is the inverse of a in $\mathbb{Z}_n$. On the other hand, if $\gcd(a, n) = d > 1$, then

$$a \times \frac{n}{d} = \frac{a}{d} \times n \equiv 0 \bmod n. \tag{1.6.5}$$

This shows that a cannot have an inverse in $\mathbb{Z}_n$. □

Note 1.6.2. The collection of invertible elements in $\mathbb{Z}_n$ is denoted by $\mathbb{Z}_n^\times$. The cardinality of this set is given by **Euler's totient function** $\varphi(n)$; that is,

$$\varphi(n) = \left|\{a : 1 \leq a \leq n \text{ and } \gcd(a,n) = 1\}\right|. \tag{1.6.6}$$

The set $\mathbb{Z}_n^\times$ is closed under multiplication and

$$\text{Inv}(x) := x^{-1} \tag{1.6.7}$$

maps $\mathbb{Z}_n^\times$ onto itself. If the context is clear, the inverse of x is written as $\frac{1}{x}$. Therefore, in $\mathbb{Z}_n$, the expression $\frac{a}{b}$ should be understood as ab^{-1}.

Exercise 1.6.3. Prove that inversion is one-to-one and onto.

This last exercise has interesting consequences. For example, if n is a prime, then $\mathbb{Z}_n^\times = \{1, 2, \ldots, n-1\}$ and adding all its elements gives

$$\sum_{j=1}^{n-1} \frac{1}{j} \equiv \sum_{j=1}^{n-1} j \mod n. \tag{1.6.8}$$

The left-hand side is the **harmonic number** H_{n-1} and the right-hand side sums to $n(n-1)/2$, an integer multiple of the odd prime n. The conclusion is that, for n prime, the numerator of the harmonic number H_{n-1} is divisible by n. This is discussed in Section 11.11.

1.7. Prime numbers

The study of **prime numbers** has interested mathematicians, professional and amateur, since the time of Euclid. The subject is rich in interesting problems that are easy to describe and (sometimes very) hard to prove. Aside from the textbooks quoted earlier, the reader is referred to the books by T. Apostol [**26**], B. Fine and G. Rosenberger [**128**], and J. Stopple [**282**] as sources that the author has enjoyed.

In this section some elementary properties of prime numbers are reviewed. In order to motivate the kind of questions considered in future chapters, the notion of **valuation** is introduced.

Definition 1.7.1. Let p be a prime and let $x \in \mathbb{Z}$. The **p-adic valuation of** x, in the case $x \neq 0$, is the largest nonnegative integer

m such that p^m divides x. The valuation of $x = 0$ is declared to be $+\infty$. The p-adic valuation of x is denoted by $\nu_p(x)$.

Note 1.7.2. Elementary properties of the valuation ν_p include the following:

(1) The statement p divides n is equivalent to $\nu_p(n) > 0$.

(2) $\nu_p(n)$ satisfies the statement: $p^{\nu_p(n)}$ divides n but $p^{\nu_p(n)+1}$ does not.

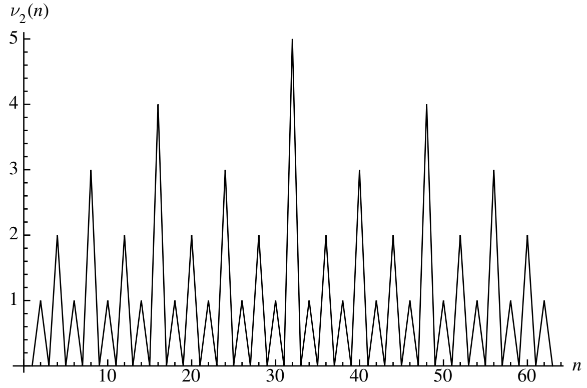


Figure 1.7.1. The 2-adic valuation of n.

Note 1.7.3. The description of the function $\nu_2(n)$ is now given in terms of a **valuation tree**. This concept will reappear in later chapters. The construction of the tree consists of a sequence of steps:

(1) The valuation tree begins with a **root**, placed at the top, that represents the set $\mathbb{N}$.

(2) For each node that has not been labeled, ask the question: *is the value of the function being considered constant at this node*? If the answer is *yes*, the node is labeled with this constant value. If the answer is *no*, then the node has to be *split*. In the first case, at the root, the function $\nu_2(n)$ is not constant, so the answer is clearly *no*.

(3) The root is then divided by a **splitting parameter**. In this case, this is 2, so the root obtains *two* vertices descending from it.

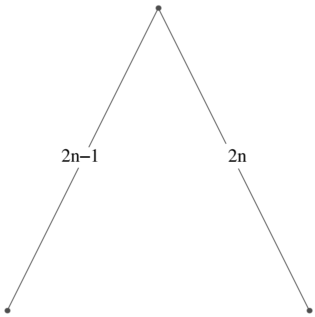


Figure 1.7.2. The 2-adic valuation n (first tree).

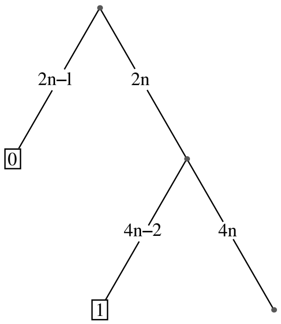


Figure 1.7.3. The 2-adic valuation n (second tree).

Each vertex corresponds to a different class modulo 2. Each valuation tree has its own splitting parameter. At this point this parameter is determined empirically, one example at the time.

The vertex on the left represents the set $\{2n - 1 : n \in \mathbb{N}\}$. Therefore, for this vertex, the question above has a positive response, with $\nu_2(2n-1) = 0$. Then the vertex is labeled 0. The same question is still negative for the second vertex, which represents the set $\{2n : n \in \mathbb{N}\}$. This vertex is now split again into two new vertices: one for $\{4n-2 : n \in \mathbb{N}\}$ and the second one for $\{4n : n \in \mathbb{N}\}$. This is depicted in Figure 1.7.3. The process is continued and the resulting tree is called the 2-adic valuation tree of the sequence $\{n : n \in \mathbb{N}\}$.

One of the points of view described in this text is that given an integer sequence a_n, its p-adic valuation $\nu_p(a_n)$ often has hidden beauty that deserves to be explored.

As an example, Figure 1.7.4 shows the function $\nu_3(n) - \nu_3(F_n)$, comparing the valuations of a Fibonacci number F_n with that of n. A computation of $\nu_5(F_n)$ shows that $\nu_5(F_n) = \nu_5(n)$. This is established in Theorem 3.5.9. Figure 1.7.5 depicts the 2-adic valuation of the Stirling numbers of the second kind $S(n,k)$, for $k = 195$. Chapter 7 provides a description of this phenomenon. The intrinsic beauty of the figure remains to be explained.

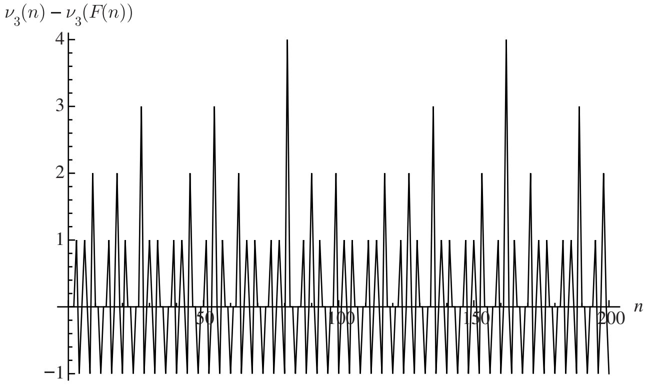


Figure 1.7.4. The function $\nu_3(n) - \nu_3(F_n)$.

Arithmetic deals with properties of integers related to divisibility. The **fundamental theorem of arithmetic**, established in Theorem 1.7.4, states that any positive integer can be expressed in a unique way as a product of prime powers. In this section the elementary parts of the subject are reviewed.

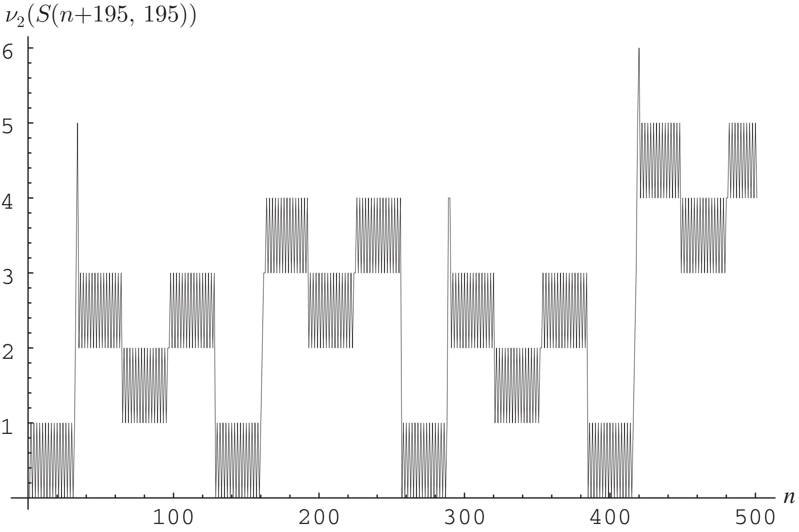


Figure 1.7.5. The power of 2 that divides the Stirling number $S(n+195, 195)$.

The set of prime numbers begins with

$$\mathbb{P} = \{2,\ 3,\ 5,\ 7,\ 11,\ 13,\ 17,\ \ldots\}, \tag{1.7.1}$$

and the first natural question that occurs is how to decide if $n \in \mathbb{N}$ is a prime number. An efficient answer to thus question turns out to be surprisingly difficult. The classical **sieve of Eratosthenes** determines the primality of numbers by making a list of all numbers up to n and then crossing out the multiples of all primes up to n. The primes are the elements of the list that do not get crossed out. This is inefficient. One of the basic questions of number theory is to develop an algorithm that decides if n is prime and it takes a number of steps that is at most a polynomial function of the number of digits of n, that is, a polynomial in $\log n$. These are called **polynomial-time algorithms**. M. Agrawal, N. Kayal, and N. Saxena [**3**] have very recently (the paper appeared in 2004) provided such an algorithm with running time proportional to $(\log n)^{15/2}$. This is a remarkable result. A very nice description of these issues is given by A. Granville in [**146**].

An even more naive approach to determine the primality of n is this: divide the number n by every integer $k \leq n$. This generates a sequence of n remainders and if none of them are zero, then n is prime.

First improvement. Instead of dividing by all integers $k \leq n$, it suffices to divide up to $k \leq \sqrt{n}$. This is clear: if $n = a \cdot b$, then one of a or b has to be in the range $\{2, \ldots, \lfloor\sqrt{n}\rfloor\}$.

Second improvement. Consider the list of primes

$$p_1 = 2, \quad p_2 = 3, \quad p_3 = 5, \ldots. \tag{1.7.2}$$

Then a number n is prime if it is not divisible by any prime $p_j \leq \sqrt{n}$. The drawback of this is that it requires us to have a list of all the primes up to $\sqrt{n}$.

1.7.1. Prime factorization of integers.

The fundamental theorem of arithmetic states that prime numbers are the basic building blocks of integers.

Theorem 1.7.4. *Any nonzero integer n can be written in the form*

$$n = \pm p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}, \tag{1.7.3}$$

where the p_i are distinct primes and $a_i \in \mathbb{N}$. This representation is unique up to rearranging of the order.

Proof. The proof of existence is an easy induction argument. Indeed, assume such a representation exists for every integer strictly less than n. In the case n is prime, then n is its own representation. If n factors as $a \cdot b$, with a, $b < n$, then collecting the representation of a and b gives that of n. The question of uniqueness is more delicate. The standard proof is based on the fact that if a prime p divides a product $a \cdot b$, then it must divide one of the factors. This is Exercise 1.5.6. Under this assumption uniqueness is clear. □

Exercise 1.7.5. Check the details. **Hint:** Use the Euclidean algorithm described in Section 1.5 to prove that if p divides $a \cdot b$ and does not divide a, then it must divide b.

Note 1.7.6. The number a_i in (1.7.3) is the p_i-adic valuation of n; that is, $a_i = \nu_{p_i}(n)$.

1.7.2. The infinitude of primes. In this section some proofs of Euclid's result that there are infinitely many primes are presented.

Theorem 1.7.7. *The set of prime numbers is infinite.*

Proof. Suppose $\mathbb{P} = \{p_1, p_2, \ldots, p_n\}$ is a complete list of all primes. Then the number $P_n = p_1 p_2 \cdots p_n + 1$ is not divisible by any element of $\mathbb{P}$ because any such divisor would divide the difference $P_n - p_1 p_2 \cdots p_n = 1$. This contradicts Theorem 1.4.6. □

The next result gives a criterion, due to S. P. Mohanty [**220**], that will be used to give another proof of Theorem 1.7.7.

Proposition 1.7.8. *Assume there is an infinite set of positive integers A such that* $\gcd(a, b) = 1$ *if a, $b \in A$ and $a \neq b$. Then there are infinitely many primes.*

Proof. The fact that the elements of A are relatively prime shows that each element of A is divisible by a different prime. This is impossible if there are only finitely many prime numbers. □

The next result shows how to produce sequences that satisfy the hypothesis of Proposition 1.7.8.

Lemma 1.7.9. *Let a and m be relatively prime numbers. Define the sequence A_n by*

$$\begin{aligned} A_0 &= a + m, \\ A_{n+1} &= A_n^2 - mA_n + m. \end{aligned}$$

Then $\gcd(A_n, A_m) = 1$ *if $n \neq m$.*

Proof. An easy induction argument shows that

$$A_n = aA_0A_1 \cdots A_{n-1} + m \tag{1.7.4}$$

and thus

$$A_n \equiv a^{2^n} \text{ mod } m. \tag{1.7.5}$$

Moreover (1.7.4) shows that the set $\{A_n : n \in \mathbb{N}\}$ is infinite. Let d be a common divisor of A_i and A_j. Then, assuming $j > i$ and using

$$A_j = aA_0 A_1 \cdots A_i \cdots A_{j-1} + m, \tag{1.7.6}$$

it follows that d divides m. Then (1.7.5) implies d also divides a power of a. It follows that d divides $\gcd(a, m) = 1$, so it must be 1. □

Note 1.7.10. The special case of $a = 1$ and $m = 2$ produces the numbers $f_n = 2^{2^n} + 1$. These are the **Fermat numbers** that satisfy the recurrence

$$f_{n+1} = f_n^2 - 2f_n + 2 \quad \text{with } f_0 = 3.$$

In this case, the proof is due to G. Polya.

1.7.3. Primes and sums of squares.

There are many beautiful connections between prime numbers and other sequences. The question of the representation of primes by a given polynomial in several variables is such an example. Dirichlet proved that, given a, $b \in \mathbb{N}$ with $\gcd(a, b) = 1$, the polynomial $f_{a,b}(x) = ax + b$ attains infinitely many primes. The reader will find an outline of the proof in the text by S. J. Miller and R. Takloo-Bighash [**218**]. The study of this question for quadratic polynomials is described in the text by D. Cox [**106**].

This section discussed the question of representations of primes as sums of two squares. This can be phrased in terms of solving the equation

$$x^2 + y^2 = p \tag{1.7.7}$$

for x, $y \in \mathbb{N}$. Naturally if (x, y) is a solution, so are $(-x, y)$, $(x, -y)$, and $(-x, -y)$. Here p denotes a fixed prime.

The case $p = 2$ is elementary: $x = y = 1$ are the only solutions. Now consider the case of an odd prime. A necessary condition for the existence of a solution is easy to produce.

Lemma 1.7.11. *Let p be an odd prime and assume p is a sum of two squares. Then p is congruent to* 1 *modulo* 4.

Proof. The squares modulo 4 are 0 and 1. There is no combination of these values that adds up to 3 modulo 4. □

P. Fermat proved that the converse is true. D. Zagier's [**317**] remarkable proof of this result is presented next. The reader will find other proofs in the text by J. H. Silverman [**274**].

Theorem 1.7.12. *Every prime* $p \equiv 1 \bmod 4$ *can be written as a sum of two squares.*

Proof. Let $p \in \mathbb{N}$ be a fixed prime number and consider the set $S := \{(x, y, z) \in \mathbb{N}^3 : x^2 + 4yz = p\}$. Define

$$\psi(x,y,z) = \begin{cases} (x+2z, z, y-x-z) & \text{if } x < y-z, \\ (2y-x, y, x-y+z) & \text{if } y-z < x < 2y, \\ (x-2y, x-y+z, y) & \text{if } x > 2y. \end{cases}$$

The set S is finite and invariant under the map ψ; that is, $\psi(S) \subset S$. To check this, let $(x, y, z) \in S$ and assume $x > 2y$. Then

$$(x-2y)^2 + 4(x-y+z)y = x^2 + 4yz = p.$$

Therefore $\psi(x, y, z) \in S$. The other cases are treated similarly.

Lemma 1.7.13. *The map* ψ *has a fixed point precisely when* $p = 4m + 1$. *Morever, if* $p \equiv 1 \bmod 4$, *then* ψ *has a unique fixed point.*

Proof. Let (x, y, z) satisfy $\psi(x, y, z) = (x, y, z)$. If $x < y - z$, then the first coordinate yields $x + 2z = x$ and this is impossible. If $y - z < x < 2y$, then the last coordinate implies $x = y$ and there are no other restrictions. The defining equation yields $x(x + 4z) = p$ and this implies $x = y = 1$ and $z = m$ is the fixed point. The reader can now study the other two cases. □

Exercise 1.7.14. Check that the map ψ is an involution, that is, $\psi \circ \psi$ is the identity.

Now partition the set S into sets of the form $\{P, \psi(P)\}$, with $P \in S$. Every such set, except the one corresponding to the fixed point $(1, 1, m)$, has two elements. It follows that S must have an odd number of elements.

Exercise 1.7.15. Assume X is a finite set with an odd number of elements. Prove that any involution $\lambda : X \to X$ must have at least one fixed point.

Now define $\lambda(x, y, z) = (x, z, y)$ for $(x, y, z) \in S$. This is an involution and Exercise 1.7.15 guarantees the existence of a fixed point for λ. This element of S must be of the form (a, b, b). This implies $a^2 + (2b)^2 = p$. This is the desired representation of p as a sum of two squares. □

1.8. The rational numbers

The set of integers $\mathbb{Z}$ was described as the set of numbers created in order to solve certain equations, such as $x + 2 = 1$, that have no solutions in $\mathbb{N}$. The set $\mathbb{Q}$ of **rational numbers** can be constructed in a similar manner as solutions of the equation $bx = a$, with a, $b \in \mathbb{Z}$ and $b \neq 0$. The solution of this equation is denoted by $\frac{a}{b}$.

An alternative definition of $\mathbb{Q}$ is given in the next exercise.

Exercise 1.8.1. Let X be the set of pairs (a, b), with a, $b \in \mathbb{Z}$ and $b \neq 0$. Define the relation $(a, b) \sim (c, d)$ by $ad = bc$. Prove that this is an equivalence relation and identify $\mathbb{Q}$ as the quotient $\mathbb{Z} \times \mathbb{Z}/\sim$. Conclude that

$$\frac{a}{b} = \frac{c}{d} \text{ in } \mathbb{Q} \text{ if and only if } ad = bc \text{ in } \mathbb{Z}.$$

Exercise 1.8.2. Define the addition of rational numbers in the usual manner:

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}. \tag{1.8.1}$$

Convince yourself that this is well-defined. Naturally it would be simpler if addition were to be defined by

$$\frac{a}{b} \oplus \frac{c}{d} = \frac{a + c}{b + d}. \tag{1.8.2}$$

Discuss the difficulties associated with this definition. Nevertheless (1.8.2) has some interesting mathematics behind it; see Definition 10.2.8.

In the representation $x = \dfrac{a}{b}$ one may assume that the integers a and b are relatively prime. This is the basic representation of rational numbers. The exercises provide a sample of others.

Exercise 1.8.3. Check that every nonzero rational number r has a prime factorization of the form

$$r = \pm p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n} \tag{1.8.3}$$

where the p_i are primes and $a_i \in \mathbb{Z}$.

The next theorem characterizes rational numbers from the point of view of their **decimal expansions** and generalizations to other bases. The proof of the theorem begins with a preliminary exercise.

Exercise 1.8.4. Let $r \in \mathbb{Q}$ and $b \in \mathbb{N}$ be fixed. Prove that r can be written in the form

$$r = \pm \sum_{k=-n}^{\infty} \frac{a_k}{b^k}, \tag{1.8.4}$$

where $a_k \in \mathbb{N}_0 = \mathbb{N} \cup \{0\}$ and $0 \leq a_k < b$. **Hint:** Assume $r > 0$ with $r = u/v$ and $u < v$. Divide ub by v to produce $ub = s_0 + q_0 v$, with $q_0 \in \mathbb{N}$ and $0 \leq s_0 < v$. Then

$$\frac{u}{v} = \frac{1}{b}\left[q_0 + \frac{s_0}{v}\right] = \frac{q_0}{b} + \frac{1}{b}\frac{s_0}{v}.$$

Now write

$$\frac{u}{v} = \frac{q_0}{b} + \frac{1}{b^2}\frac{s_0 b}{v}$$

and divide $s_0 b$ by v to continue the process.

Note 1.8.5. In order to be completely honest, it has to be stated that the infinite sum in (1.8.4) has not been defined. An alternative approach is this: prove that for $r \in \mathbb{Q}$ there is a sequence of integers a_k, with $0 \leq a_k < b$, such that the sum $\sum_{k=-n}^{m} a_k/b^k$ can be arbitrarily close to r by choosing m large enough.

The main result in this section is stated next.

Theorem 1.8.6. *Let $b \in \mathbb{N}$ and $a_k \in \mathbb{N}$ with $0 \leq a_k < b$. Any series of the form* (1.8.4) *is a rational number if and only if the sequence $\{a_k\}$ is eventually periodic. That is, there is an index j such that for $k \geq j$, the sequence $\{a_k\}$ is periodic.*

Proof. Given a series satisfying the stated conditions, subtract the terms with negative index and those appearing before j, to assume that

$$x = \sum_{k=0}^{\infty} \frac{a_k}{b^k} \tag{1.8.5}$$

with a_k of period ℓ. Divide k by ℓ to produce $k = q\ell + j$, with $0 \leq j \leq \ell$. Use periodicity to conclude that $a_k = a_j$. Then

$$\begin{aligned} x &= \sum_{k=0}^{\infty} \frac{a_k}{b^k} \\ &= \sum_{q=0}^{\infty} \sum_{j=0}^{\ell-1} \frac{a_j}{b^{q\ell+j}} \\ &= \sum_{q=0}^{\infty} \frac{1}{b^{q\ell}} \times \sum_{j=0}^{\ell-1} \frac{a_j}{b^j}. \end{aligned}$$

Define

$$y = \sum_{j=0}^{\ell-1} \frac{a_j}{b^j} \tag{1.8.6}$$

and sum the geometric series as in Exercise 1.5.17 to obtain

$$r = \frac{y\, b^\ell}{b^\ell - 1}. \tag{1.8.7}$$

This shows that r is a rational number. □

Exercise 1.8.7. Prove the converse to complete the proof.

Note 1.8.8. Section 1.9 describes the fact that any *real number* x can be represented (in an essentially unique way) in the form

$$x = \sum_{k=-n}^{\infty} \frac{a_k}{b^k} \tag{1.8.8}$$

where $b > 1$ is a fixed integer, called the **base**, and for integers a_k, with $0 \leq a_k \leq b - 1$, called the **digits of** x **in base** b. This extends the usual **decimal expansion**. From this point of view, it is quite easy to produce real numbers that are not rational: simply take a nonperiodic sequence $\{a_k\}$.

Note 1.8.9. The number $x = \sum_{k=1}^{\infty} a_k$, with

$$a_k = \begin{cases} 10^{-n} & \text{if } n = k^2, \\ -10^{-n} & \text{otherwise} \end{cases} \tag{1.8.9}$$

has recently been shown to be irrational in a paper by J. Villa-Morales [**300**]. This is not quite a decimal expansion, since $a_k < 0$ is allowed.

Note 1.8.10. The literature contains a variety of interesting irrational numbers. G. Dresden [**113, 114**] has given some examples. Let $f : \mathbb{N} \to \mathbb{N}$ be a function and denote by $\texttt{lnzd}(f(n))$ the last nonzero digit of $f(n)$. To each such f associate the real number

$$x(f) = 0.d_1d_2d_3 \ldots d_n \ldots$$

with $d_n = \texttt{lnzd}(f(n))$. G. Dresden has shown that $x(n!)$ and $x(n^n)$ are irrational numbers.

1.8.1. The cardinality of $\mathbb{Q}$. The notion of **cardinality** of a finite set has a clear intuitive meaning. It should not surprise the reader that the transition from this level to a more rigorous definition is difficult. R. Dedekind declared a set M to be **infinite** if there exists a function $f : M \to M$ that is one-to-one but not onto. The successor function shows that $\mathbb{N}$ is infinite (no surprises here!). It can be shown that the existence of an infinite set is equivalent to the existence of a set with a function satisfying the rules of successors given above. The reader will find more details on these issues in the book by H. Ebbinhaus et al. [**120**]. The current text deals with these issues in a very intuitive manner.

The cardinality of a **finite** set F is the unique $n \in \mathbb{N}$ such that there is a bijective (one-to-one and onto) correspondence $\psi : F \to A_n$ with a set of the form

$$A_n = \{1, 2, 3, \ldots, n\}. \tag{1.8.10}$$

Using this correspondence, the set F can be written in the form $\{x_1, x_2, x_3, \ldots, x_n\}$, with $\psi(x_i) = i$.

This principle can be extended to those infinite sets for which one can establish a correspondence with $\mathbb{N}$.

Definition 1.8.11. A set C is called **countable** if there is a function $\psi : C \to \mathbb{N}$ that is one-to-one and onto. The set C can now be listed as

$$C = \{x_1, x_2, x_3, \ldots\} \tag{1.8.11}$$

where $\psi(x_i) = i$ for $i \in \mathbb{N}$. The function ψ counts the elements of C.

Note 1.8.12. Every infinite set X contains a countable subset C. This subset is produced by taking an element $x_1 \in X$ and declaring it to be the first element of C. Then continue this process with the set $X - \{x_1\}$. The formalization of this construction requires the **axiom of choice**.

The question of counting infinite sets is sometimes nonintuitive. The next exercises show some examples and they will be used to prove that the set of **rational numbers** is countable. It follows that there is a bijection $\psi : \mathbb{N} \to \mathbb{Q}$. Thus, there are as many natural numbers as rational ones. **This is a highly nonintuitive result**.

Exercise 1.8.13. Prove that the set $\mathbb{N} \times \mathbb{N}$ is countable. **Hint:** Consider the function $f(a, b) = 2^{a-1}(2b - 1)$.

Exercise 1.8.14. Prove that a finite union of countable sets is countable. The same is true for a countable union of finite sets.

The next exercise provides an interesting way to prove countability of a set.

Exercise 1.8.15. Let X be a set and let $h : X \to \mathbb{N}$ be a function such that for each $n \in \mathbb{N}$ the set

$$X_n := \{x \in X : h(x) < n\} \tag{1.8.12}$$

is finite. Prove that X is countable. The function h is called a **height** for X.

The cardinality of $\mathbb{Q}$ is established next.

Theorem 1.8.16. *The set $\mathbb{Q}$ is countable.*

Proof. Let $r = \frac{m}{n} \in \mathbb{Q}$, with $\gcd(m, n) = 1$. Define the **height** of r by $h(r) = |m| + |n|$. Then

$$\mathbb{Q} = \bigcup_{j=1}^{\infty} \{r \in \mathbb{Q} : h(r) = j\}.$$

The function h satisfies the conditions of Exercise 1.8.15. □

Exercise 1.8.17. Prove that $\mathbb{Z} \times \mathbb{Z}$ is countable. **Hint:** Use Exercise 1.8.13. Conclude that $\mathbb{Q}$ is countable by exhibiting a map $\psi : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Q}$.

Exercise 1.8.18. This exercise outlines the proof of countability of $\mathbb{Q}$ based on the **diagonal procedure** due to G. Cantor. Consider first the set of positive rationals. Now make an array of the form

$$\begin{array}{cccccc}
\frac{1}{1} & \frac{2}{1} & \frac{3}{1} & \frac{4}{1} & \frac{5}{1} & \frac{6}{1} \cdots \\
\frac{1}{2} & \frac{2}{2} & \frac{3}{2} & \frac{4}{2} & \frac{5}{2} & \frac{6}{2} \cdots \\
\frac{1}{3} & \frac{2}{3} & \frac{3}{3} & \frac{4}{3} & \frac{5}{3} & \frac{6}{3} \cdots \\
\frac{1}{4} & \frac{2}{4} & \frac{3}{4} & \frac{4}{4} & \frac{5}{4} & \frac{6}{4} \cdots
\end{array}$$

that contains all positive rational numbers. Arrange them on a single line by marching along the diagonals as in

$$\frac{1}{1}, \frac{2}{1}, \frac{1}{2}, \frac{3}{1}, \frac{2}{2}, \frac{1}{3}, \frac{4}{1}, \frac{3}{2}, \frac{2}{3}, \frac{1}{4}, \frac{5}{1}, \frac{4}{2}, \frac{3}{3}, \frac{2}{4}, \frac{1}{5}, \cdots$$

and then delete the repeated values to produce

$$\frac{1}{1}, \frac{2}{1}, \frac{1}{2}, \frac{3}{1}, \frac{1}{3}, \frac{4}{1}, \frac{3}{2}, \frac{2}{3}, \frac{1}{4}, \frac{5}{1}, \frac{1}{5}, \cdots .$$

This gives a bijection between $\mathbb{Q}^+$ and $\mathbb{N}$. Write the list of positive rationals as $\{x_1, x_2, x_3, \ldots\}$. Repeat for the negative rationals to produce a second list $\{y_1, y_2, y_3, \ldots\}$. Now interlace both lists and add 0 to produce $\{0, x_1, y_1, x_2, y_2, \ldots\}$ and the countability of $\mathbb{Q}$.

The next exercise provides a proof that $\mathbb{Q}$ is countable due to Y. Sagher [**264**]. It employs the unique factorization of an integer into primes.

Exercise 1.8.19. Let m, $n \in \mathbb{N}$ be relatively prime. Assume that

$$m = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k} \quad \text{and} \quad n = q_1^{b_1} q_2^{b_2} \cdots q_l^{b_l}$$

are their respective prime factorizations. Define $f(1) = 1$ and

$$f\left(\frac{m}{n}\right) = p_1^{2a_1} p_2^{2a_2} \cdots p_k^{2a_k} q_1^{2b_1-1} \cdots q_l^{2b_l-1}$$

for $m \neq n$. Prove that f is one-to-one and onto $\mathbb{N}$.

Note 1.8.20. The article by D. Bradley [**75**] contains a survey of the many proofs of countability of $\mathbb{Q}$.

1.8.2. An explicit formula by N. Calkin and H. Wilf.

The diagonalization process of G. Cantor described in Exercise 1.8.18 provides a proof of the countability of $\mathbb{Q}$. The difficulty is that, due to the cancellation of repeated fractions, the location of a specific rational in the final list is hard to predict.

N. Calkin and H. Wilf [**89**] gave a new proof of Theorem 1.8.16 by exhibiting an explicit enumeration in one direction; i.e., given an index n, they produce a formula that gives the nth rational. The procedure starts with a binary tree with rational numbers assigned to each vertex. The top vertex is $\frac{1}{1}$. Each vertex with label $\frac{m}{n}$ has two children: its left child is $\frac{m}{m+n}$ and its right child is $\frac{m+n}{n}$. Now make a list by starting at the top vertex and moving down along the tree reading from left to right:

$$\mathbb{L} = \left\{ \frac{1}{1}, \frac{1}{2}, \frac{2}{1}, \frac{1}{3}, \frac{3}{2}, \frac{2}{3}, \frac{3}{1}, \frac{1}{4}, \frac{4}{3}, \frac{3}{5}, \frac{5}{2}, \frac{2}{5}, \frac{5}{3}, \frac{3}{4}, \frac{4}{1}, \cdots \right\}.$$

Theorem 1.8.21. *The list* $\mathbb{L}$ *satisfies the following:*

(a) *Every element is a rational number in reduced form.*

(b) *Every reduced positive rational number occurs exactly once in* $\mathbb{L}$.

Therefore, $\mathbb{Q}^+$ *is countable.*

Proof. The rational label of the top vertex is $1/1$, in reduced form. Let m/n be the vertex at the highest level whose label is not reduced. If m/n is a left child, then its parent is $m/(n-m)$, which would not be reduced. Similarly, if m/n is a right child, its parent is $(m-n)/n$, not reduced either. This contradicts the highest level assumption on m/n and establishes part (a).

To prove (b), it is established that if a fraction is missing, then so is its parent. This can be traced up to $1/1$ to obtain a contradiction. Let m/n be a fraction with the smallest denominator that is missing from the list. In case there are many missing fractions with denominator n, take m to be the smallest among the corresponding numerators. If $m > n$, then $(m-n)/n$ is not in the list, because its child m/n is missing. But this fraction has denominator n and numerator smaller than m. It follows that $(m-n)/n$, the parent of m/n, is also missing. The same works if $m < n$ with its parent $m/(n-m)$. Therefore every positive rational occurs at least once in the list. The uniqueness is established by a similar argument applied to the rational number of the minimal denominator that has two appearances in the list. □

Note 1.8.22. A proof of the Calkin-Wilf enumeration principle has been given by D. Callan. This is presented in Note 1.8.27.

Note 1.8.23. Observe that in the list created above the denominator of each fraction is the numerator of its successor. Check it. It follows that the list $\mathbb{L}$ can be expressed in the form

$$\mathbb{L} = \left\{ \frac{f(n)}{f(n+1)} \, : \, n \geq 0 \right\} \tag{1.8.13}$$

for some function f. The rules of formation of the list produce

$$f(2n+1) = f(n) \text{ and } f(2n+2) = f(n)+f(n+1), \text{ for } n \geq 0. \tag{1.8.14}$$

The paper by N. Calkin and H. Wilf [**89**] shows that $f(n)$ counts the number of ways to write n as a sum of powers of 2, each power being used at most twice. The authors of [**89**] called $f(n)$ the number of **hyperbinary representation** of n.

Note 1.8.24. Figure 1.8.1 shows the function f for $1 \leq n \leq 2^{14}$.

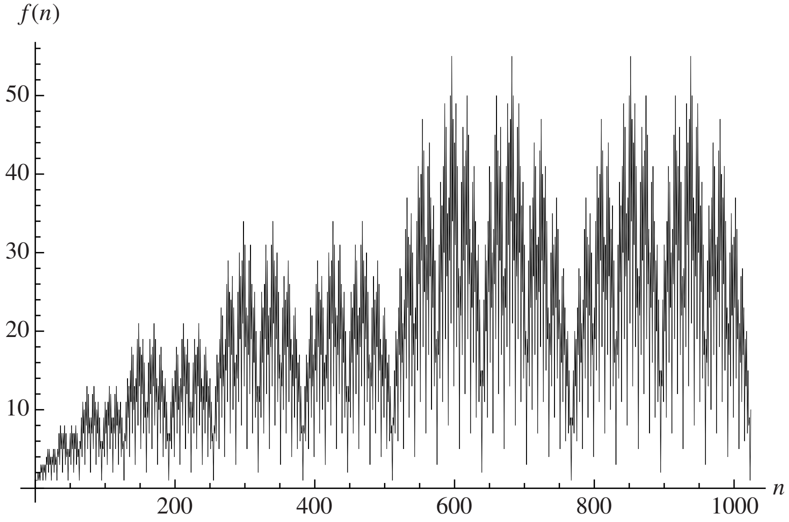


Figure 1.8.1. The Calkin-Wilf function.

1.8.3. Approximation of rational numbers. The **decimal expansion** of a rational number α was described in Note 1.8.8. This expansion is the special case of $b = 10$ of the result in Exercise 1.8.4. The expansion is now employed to obtain an interesting form of approximating $\alpha \in \mathbb{Q}$. The general procedure is illustrated with an example. Let

$$\alpha = \frac{78539823}{25000000} \sim 3.14159292000, \tag{1.8.15}$$

which the reader will recognize as an approximation to π.

The Euclidean algorithm applied to the numbers 78539823 and 25000000 gives

$$\begin{aligned}
78539823 &= 3 \times 25000000 + 3539823 \\
25000000 &= 7 \times 3539823 + 221239 \\
3539823 &= 15 \times 221239 + 221238 \\
221239 &= 1 \times 221238 + 1.
\end{aligned}$$

This confirms that the fraction α is in reduced form.

Now write

$$\begin{aligned}\frac{78539823}{25000000} &= 3+\cfrac{1}{\cfrac{25000000}{3539823}} = 3+\cfrac{1}{7+\cfrac{1}{\cfrac{3539823}{221238}}}\\ &= 3+\cfrac{1}{7+\cfrac{1}{15+\cfrac{1}{\cfrac{221239}{221238}}}} = 3+\cfrac{1}{7+\cfrac{1}{15+\cfrac{1}{1+\cfrac{1}{221238}}}}.\end{aligned}$$

The fraction 1/221238 is very small, so a good approximation to α is obtained by dropping it. This yields

$$\alpha \sim \beta = 3+\cfrac{1}{7+\cfrac{1}{15+\cfrac{1}{1}}} = \frac{355}{113}.$$

What is surprising is that one gets a very good approximation to α with a rational number that is the quotient of two relatively small numbers. Indeed,

$$\beta = \frac{355}{113} \sim 3.14159292035$$

and

$$\left|\frac{78539823}{25000000} - \frac{355}{113}\right| < 10^{-9}.$$

Exercise 1.8.25. The first two terms in the expansion for α give $\alpha \sim \frac{22}{7}$. In Chapter 12 it will be shown that π is not rational, so $\pi \neq \frac{22}{7}$. Verify this by evaluating the integral

$$\int_0^1 \frac{x^4(1-x)^4}{1+x^2}\,dx = \frac{22}{7} - \pi.$$

This example appears in D. P. Dalzell [**108**], but the original formulation of this evaluation is not known to the author. Information about this would be appreciated. The reader will find in S. K. Lucas [**205**] the evaluations

$$\int_0^1 \frac{x^5(1-x)^6(197+462x^2)}{530(1+x^2)}\,dx = \pi - \frac{333}{106}$$

and

$$\int_0^1 \frac{x^8(1-x)^8(25+816x^2)}{3164(1+x^2)}\,dx = \frac{355}{113} - \pi.$$

Note 1.8.26. The approximations for α given above are now explained in terms of **continued fractions**. The process begins with the Euclidean algorithm: given two positive integers a, b, generate the sequence of quotients and remainders as in (1.5.3) starting at $r_0 = a$ and $r_1 = b$ and continuing with

$$\begin{aligned} r_0 &= r_1 q_1 + r_2, \quad 0 \leq r_2 < r_1, \\ r_1 &= r_2 q_2 + r_3, \quad 0 \leq r_3 < r_2, \\ \cdots &= \cdots \\ r_{n-2} &= r_{n-1} q_{n-1} + r_n, \quad 0 \leq r_n < r_{n-1}, \\ r_{n-1} &= r_n q_n. \end{aligned}$$

Now write $a = bq_1 + r_2$ as

$$\frac{a}{b} = q_1 + \frac{r_2}{b} = q_1 + \frac{1}{\dfrac{b}{r_2}}.$$

Continue with $b = r_2 q_2 + r_3$ to write

$$\begin{aligned} \frac{a}{b} &= q_1 + \frac{r_2}{b} \\ &= q_1 + \frac{1}{\dfrac{b}{r_2}} \\ &= q_1 + \frac{1}{q_2 + \dfrac{1}{\dfrac{r_2}{r_3}}}. \end{aligned}$$

This process finishes in a finite number of steps producing the **continued fraction representation** of the rational number a/b. The final result has the form

$$\frac{a}{b} = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{1}{q_4 + \cfrac{1}{\cdots + \cfrac{1}{q_n}}}}}. \tag{1.8.16}$$

More details are given in Subsection 1.9.5.

Note 1.8.27. D. Callan [**90**] has provided a one-line description of the Calkin-Wilf enumeration of the rationals given in Theorem 1.8.21. First observe that every rational number has a unique continued fraction expansion of odd length obtained by replacing the last partial quotient a_n by $a_n - 1$ if necessary. For example

$$\frac{355}{113} = 3 + \cfrac{1}{7 + \cfrac{1}{16}}.$$

Now reverse the order of the sequence of partial quotients, to produce [16, 7, 3]. Then create a binary number by producing a sequence of 1's and 0's with length given by the sequence of partial quotients described in the previous step. In the example this gives the positive integer

$$11111111111111110000000111_2 = 67107847.$$

The map that sends 355/113 to 67107847 enumerates the rationals.

1.9. The set of real numbers

The construction of number systems developed up to now has been an algebraic procedure. The initial set $\mathbb{N}$ was enlarged first by adding all solutions to equations of the form $x + a = b$, with $a, b \in \mathbb{N}$. This produces the set $\mathbb{Z}$ of integers. A small technical point has to be inforced: the equations $x+2 = 5$ and $x+3 = 6$ define the *same integer*. The passage from $\mathbb{Z}$ to the rational numbers $\mathbb{Q}$ is similar: simply add to the integers all solutions of equations of the form $ax = b$, with $a, b \in \mathbb{Z}$ and $a \neq 0$. As before, the equations $ax = b$ and $cx = d$ define the same rational number when $ad = bc$ and $a \neq 0$, $c \neq 0$.

The question that remains is what is the next step in the chain

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q}. \tag{1.9.1}$$

Are there any natural operations that cannot be performed in $\mathbb{Q}$?

The next subsection illustrates one of them.

1.9.1. The irrationality of a square root.

Recall that $b \in \mathbb{Q}^+$ is called the **square root** of $a \in \mathbb{Q}^+$ if $b^2 = a$. It is now shown that there are many numbers in $\mathbb{Q}^+$ that do not have square roots in $\mathbb{Q}$.

Theorem 1.9.1. *Let $a \in \mathbb{N}$. Suppose a is not the square of an integer. Then a does not have a square root in $\mathbb{Q}^+$; that is, there is no rational number r such that $r^2 = a$.*

Proof. Suppose that $(m/n)^2 = a$ with m, $n \in \mathbb{N}$. Write m/n with a *minimal* denominator. The number $m/n \notin \mathbb{N}$, so $m/n > 1$. Choose $q \in \mathbb{N}$ such that $q < \dfrac{m}{n} < q+1$. The identity $m^2 = an^2$ yields

$$m(m-qn) = m^2 - qmn = an^2 - qmn = n(an-qm).$$

It follows that

$$\frac{m}{n} = \frac{an-qm}{m-qn}$$

and observe that $nq < m < n(q+1)$, therefore $0 < m - qn < n$. This contradicts the minimality of n. □

Exercise 1.9.2. Give a second proof of Theorem 1.9.1 using the unique factorization of integers in terms of primes.

At this point, the natural step to continue the chain (1.9.1) is to add to $\mathbb{Q}$ the solutions to all quadratic equations with coefficients in $\mathbb{Q}$. A larger class is obtained by adding solutions to all polynomial equations at once. This produces the set of **algebraic numbers**. Theorem 4.4.17 shows that it is a countable set but, in general, it is very hard to decide if a given number is in it or not. The next section introduces the set of real numbers and the chain (1.9.1) is extended one more time.

1.9.2. The real numbers. The literature contains two possible approaches to the **real numbers** $\mathbb{R}$. The first one postulates the existence of the set of real numbers and provides a list of axioms. Then it is established that $\mathbb{R}$ contains $\mathbb{Q}$ and it has the familiar arithmetic, analytic, and order properties. The reader will find a very clear exposition of this point of view in O. Hijab [**168**] and K. R. Stromberg [**285**]. A second approach, the one preferred here, is to introduce the notion of Cauchy sequence.

Definition 1.9.3. A sequence of rational numbers $\mathbf{r} := \{r_n : n \in \mathbb{N}\}$ is called a **Cauchy sequence** if for every $\epsilon \in \mathbb{Q}^+$ there exists $k \in \mathbb{N}$ such that $|r_n - r_m| < \epsilon$ for all n, $m > k$. Naturally, the number k depends on ϵ.

In some sense, the concept of a Cauchy sequence plays the role of the algebraic equations that were employed to extend $\mathbb{N}$ to $\mathbb{Z}$ and then to $\mathbb{Q}$. As before, there are sequences that need to be identified: two Cauchy sequences $\{r_n\}$ and $\{s_n\}$ are called **equivalent** if $|r_n - s_n|$ can be made arbitrarily small for large enough n. The intuition is that these two sequences will converge to *the same number*.

Definition 1.9.4. A **real number** r is an equivalence class of Cauchy sequences of rational numbers.

Exercise 1.9.5. Prove that the series appearing in Exercise 1.8.4 is a real number for any choice of $a_k \in \mathbb{N}$. **Hint:** Consider the sequence of partial sums.

Exercise 1.9.6. Given a sequence of real numbers x_n, define the concept of convergence of x_n to a limit x.

Note 1.9.7. The set $\mathbb{R}$ is then provided with an algebraic structure. The addition and multiplication in $\mathbb{R}$ are defined, in an obvious manner, in terms of the defining sequences. The notion of **order** in $\mathbb{R}$ is introduced in a similar form. The remarkable result is that the real numbers form a **complete set**: every Cauchy sequence $\{x_n : n \in \mathbb{N}\}$ converges to an element $x \in \mathbb{R}$.

Something is lost in the passage from $\mathbb{Q}$ to $\mathbb{R}$.

Theorem 1.9.8. *The set of real numbers $\mathbb{R}$ is not countable.*

This result is due to G. Cantor. The standard proof of this theorem is based on the decimal expansions of real numbers. Details can be found in the textbooks [**168, 285**] mentioned before.

Note 1.9.9. From the point of view of cardinality, there are many more irrational real numbers than rational ones. On the other hand, to check that a specific real number is irrational could be very difficult. Some examples are included in the text. Chapter 11 contains a proof that e is irrational and Chapter 12 does the same for π. On the other hand, as of the date of writing this text (January 2012), the irrationality of $e+\pi$ has not been decided.

Example 1.9.10. The concept of Cauchy sequence is illustrated with an example. Theorem 1.9.1 has shown that if $a \in \mathbb{Q}^+$ is not the square of an integer, then it does not have a rational square root. The fact is that it has a *real square root*. The next step is to produce a sequence of rational numbers x_n such that x_n^2 becomes arbitrarily close to a.

The construction of the sequence $\{x_n \, : \, n \in \mathbb{N}\}$ is obtained by **Newton's method**. Define $f(x) = x^2 - a$. Consider the sequence defined by

$$x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)},$$

starting at $x_0 \in \mathbb{Q}$ and $x_0 > 0$. In the specific case considered here

$$x_{n+1} := \frac{1}{2}\left(x_n + \frac{a}{x_n} \right). \tag{1.9.2}$$

The goal is to estimate the difference $|x_{n+k} - x_n|$. Observe first that if x_n is such that $x_n^2 = a$, then $x_{n+k} = x_n$ for all $k \in \mathbb{N}$. Assume that $x_0^2 > a$. Then $x_n \in \mathbb{Q}$ and

$$x_{n+1} - x_n = \frac{1}{2}(x_n - x_{n-1}) \times \left(1 - \frac{a}{x_n x_{n-1}} \right).$$

Induction shows that $x_{n+1} < x_n$ and that $x_{n+1}x_n > a$. Indeed

$$x_{n+1}x_n = \frac{1}{2}(x_n^2 + a) > \frac{1}{2}(x_n x_{n-1} + a) > a,$$

and from the value of $x_{n+1} - x_n$, it follows that $x_{n+1} - x_n$ and $x_n - x_{n-1}$ have the same sign. The initial step $x_1 < x_0$ is elementary. It follows that $x_n - x_{n+1} < \frac{1}{2}(x_{n-1} - x_n)$, and $x_n - x_{n+1} < 2^{-n}(x_0 - x_1)$ is established. Finally

$$\begin{aligned} x_n - x_{n+k} &= (x_n - x_{n+1}) + (x_{n+1} - x_{n+2}) + \cdots + (x_{n+k-1} - x_{n+k}) \\ &< 2^{-n-k} + 2^{-n-k-1} + \cdots + 2^{-n-1} < 2^{-n} < 1/n. \end{aligned}$$

Exercise 1.9.11. Show that if $x_0^2 < a$, then $x_1^2 > a$ and the previous argument can be started at x_1.

The last inequality $2^{-n} < 1/n$ is equivalent to $n < 2^n$. This is easy to establish by induction. A new kind of proof, explained in the next definition, is requested in Exercise 1.9.13.

Definition 1.9.12. Given two positive integers a and b, a **combinatorial proof** that $a = b$ refers to finding two sets A and B with $|A| = a, |B| = b$, and a bijection from A to B. Similarly, to provide a combinatorial proof of the inequality $a \leq b$ means to find $f : A \to B$ that is one-to-one. The meaning of a combinatorial proof of $a < b$ is clear: find a function from A to B that is one-to-one and not onto.

Exercise 1.9.13. Give a combinatorial proof of $n < 2^n$. **Hint:** A set with n elements has 2^n subsets.

The argument above shows that $|x_n - x_m|$ can be made arbitrarily small by choosing n sufficiently large. Therefore the sequence $\{x_n\}$ defined in (1.9.2) is a Cauchy sequence, so it is a real number. This number is called **the square root of** a and is denoted by $\sqrt{a}$.

Exercise 1.9.14. Prove that $(\sqrt{a})^2 = a$. **Hint:** First read Subsection 1.9.3.

Thus, the Cauchy sequence $\{x_n\}$ is the answer to the **missing number** described in Theorem 1.9.1.

The irrationality of a real number may be detected by the rate of approximation of rational sequences. A simple criteria is presented next.

Theorem 1.9.15. *Let $\delta \in \mathbb{R}^+$. Assume there is a sequence of distinct positive rational numbers r_n/s_n (written in reduced form) such that*

$$s_n \left| \delta - \frac{r_n}{s_n} \right| \to 0,$$

as $n \to \infty$. Then δ is irrational.

Proof. Assume $\delta = p/q$ in reduced form. There is at most one index $n = n_0$ for which $\delta = r_n/s_n$. Then, for $n > n_0$, it follows that

$$s_n \left| \delta - \frac{r_n}{s_n} \right| = \frac{|ps_n - qr_n|}{q} \geq \frac{1}{q}.$$

This contradicts the assumption on s_n. □

Example 1.9.16. This example uses the previous criteria to provide a different proof of the irrationality of $\sqrt{2}$. Let $\delta = \sqrt{2}$. Construct the sequence of positive integers by

$$r_{n+1} = r_n + 2s_n \quad \text{and} \quad s_{n+1} = r_n + s_n,$$

starting at $r_0 = s_0 = 1$. An elementary induction argument gives $r_n \geq s_n$ and

$$2s_n^2 = r_n^2 + (-1)^n.$$

This yields

$$\frac{1}{s_n^2} = \left| 2 - \frac{r_n^2}{s_n^2} \right| = \left| \sqrt{2} - \frac{r_n}{s_n} \right| \cdot \left| \sqrt{2} + \frac{r_n}{s_n} \right|.$$

Therefore

$$s_n \left| \sqrt{2} - \frac{r_n}{s_n} \right| \leq s_n \left| 2 - \frac{r_n^2}{s_n^2} \right| \leq \frac{1}{s_n} \to 0.$$

It follows that $\sqrt{2} \notin \mathbb{Q}$.

1.9.3. Operations with real numbers. The standard arithmetical operations on real numbers are defined in terms of the Cauchy sequences defining them. For example, if $\mathbf{a} = (a_n)$ and $\mathbf{b} = (b_n)$ are real numbers, then the sequence $(a_n + b_n)$ is a Cauchy sequence of rational numbers. This is defined to be $\mathbf{a} + \mathbf{b}$. Similar expressions define the product $\mathbf{a} \cdot \mathbf{b}$, reciprocal $1/\mathbf{a}$ for $\mathbf{a} \neq 0$, and exponentiation $\mathbf{a}^{\mathbf{b}}$ for $\mathbf{a} \geq 0$.

Note 1.9.17. The arithmetic questions of real numbers turn out to be surprisingly difficult. Theorem 1.9.8 states that the set of real numbers is **uncountable**, so most real numbers are irrational. It is a different issue to check that a specific number is not rational. The fact that $\sqrt{2} \notin \mathbb{Q}$ has been established here. This can be used to prove the result that *there are* a, $b \notin \mathbb{Q}$ *such that* $a^b \in \mathbb{Q}$. Indeed, if $\sqrt{2}^{\sqrt{2}} \in \mathbb{Q}$, then the result holds. If not, the irrational number $a = \sqrt{2}^{\sqrt{2}}$ satisfies $a^{\sqrt{2}} = 2 \in \mathbb{Q}$. It is a difficult result that the latter case is the true one.

1.9.4. Square roots and improvements to convergence. The values of functions defined in future chapters are obtained by following an informal approach. Naturally it is possible to proceed in a more rigorous fashion. This point of view is illustrated with the *square root function* $f(x) = \sqrt{x}$.

The starting point is $x \in \mathbb{R}^+$. This yields a sequence $x_n \in \mathbb{Q}^+$ that defines x. Now fix $n \in \mathbb{N}$ and produce a sequence $y_{m,n}$ that defines the square root $\sqrt{x_n}$. Then one shows that $y_{m,n}$ yields a Cauchy sequence that defines $\sqrt{x}$. An alternative to this procedure, employing power series, will be described in Chapter 2.

Note 1.9.18. Given a sequence $\{x_n\}$ that converges to $x \in \mathbb{R}$, the estimates of the **error term** $\epsilon_n := x_n - x$ are indicators of the speed of the convergence. The analysis for the sequence $\{x_n\}$ given in Example 1.9.10 is presented next. Define the error term

$$\epsilon_n := x_n - \sqrt{2}$$

and consider first the case $a = 2$. Observe that

$$\begin{aligned} \frac{1}{x_n} &= \frac{1}{\epsilon_n + \sqrt{2}} \\ &= \frac{\sqrt{2} - \epsilon_n}{2} + \frac{\epsilon_n^2}{2(\sqrt{2} + \epsilon_n)} \end{aligned}$$

from which it follows that

$$\epsilon_{n+1} = \frac{1}{2} \times \frac{\epsilon_n^2}{\sqrt{2} + \epsilon_n}.$$

Therefore $\epsilon_{n+1} \leq \frac{1}{2}\epsilon_n$ and by induction $\epsilon_n \leq \left(\frac{1}{2}\right)^n \epsilon_0$. Thus the sequence exhibits **geometric convergence**.

The general case can be obtained from the case $a = 2$ by scaling. Indeed, define

$$v_n = \frac{\sqrt{a}}{\sqrt{2}} x_n$$

and now the errors $\epsilon_n := v_n - \sqrt{a}$ satisfy

$$\begin{aligned}
\epsilon_{n+1} &= x_{n+1} - \sqrt{a} \\
&= \frac{1}{2}\left((\sqrt{a} + \epsilon_n) + \frac{a}{\sqrt{a} + \epsilon_n} \right) - \sqrt{a} \\
&= \frac{1}{2}\left(\frac{a}{\sqrt{a} + \epsilon_n} - (\sqrt{a} - \epsilon_n) \right) \\
&= \frac{1}{2} \times \frac{\epsilon_n^2}{\sqrt{a} + \epsilon_n} < \frac{1}{2}\epsilon_n,
\end{aligned}$$

and geometric convergence is observed again.

Note 1.9.19. The sequence $\{x_n\}$ converges even faster than the estimate established in the previous note. Indeed, in the last step simply bound the denominator by $\sqrt{a}$ to obtain

$$\epsilon_{n+1} \leq \frac{1}{2\sqrt{a}} \epsilon_n^2.$$

This is **quadratic convergence** and it states that near the limit the number of correct digits doubles with each step.

The next theorem provides a new sequence converging to $\sqrt{a}$ that was used by X. Gourdon and B. Salvy [**141**] to compute one million digits of $\sqrt{2}$ in Maple. It has the advantage that only divisions by 2 are required, but x_n^3 has to be evaluated. The recurrence (1.9.3) comes from applying Newton's method to the function $f(x) = 1 - a/x^2$.

Theorem 1.9.20. *The sequence*

$$x_{n+1} = \frac{3}{2} x_n - \frac{1}{2a} x_n^3 \tag{1.9.3}$$

converges to $\sqrt{a}$.

Exercise 1.9.21. Check the details. Show that it suffices to consider the case $a = 1/\sqrt{2}$. Estimate the error $\left| x_n - 1/\sqrt{2} \right|$.

1.9.5. Continued fraction representations of real numbers. The continued fraction representation of a rational number $r = a/b$ was described in Subsection 1.8.3. This procedure is now adapted to produce a similar representation for real numbers.

Start with $x \in \mathbb{R}^+$ and assume $x \notin \mathbb{N}$. Define

$$x_0 = \lfloor x \rfloor \tag{1.9.4}$$

to be the **integer part** of x. This is the unique integer m that satisfies $x - 1 < m < x$. The remainder is the **fractional part** of x defined by

$$\{x\} = x - \lfloor x \rfloor = x - x_0. \tag{1.9.5}$$

The fractional part satisfies $0 < \{x\} < 1$. Now write

$$x = \lfloor x \rfloor + \{x\} = x_0 + \cfrac{1}{\cfrac{1}{\{x\}}}.$$

The number $y = 1/\{x\}$ satisfies $y > 1$. The procedure described above can now be applied to y and iterated to obtain

$$x = x_0 + \cfrac{1}{x_1 + \cfrac{1}{x_2 + \cfrac{1}{x_3 + \cdots}}}. \tag{1.9.6}$$

This is the **continued fraction representation** of x. In order to save space, this is often written as $x = [x_0; x_1, x_2, \ldots]$. Also, the notation $[x_0, x_1, x_2, \ldots, x_n]$ is employed for the finite continued fraction

$$x_0 + \cfrac{1}{x_1 + \cfrac{1}{x_2 + \cfrac{1}{x_3 + \cfrac{1}{\cdots + \cfrac{1}{x_n}}}}}. \tag{1.9.7}$$

This fraction is written as $\dfrac{p_n}{q_n}$ and the $\dfrac{p_n}{q_n}$ are called the **convergents** of x. The numbers x_n are called the **partial quotients** of x.

Exercise 1.9.22. This exercise shows the operational rules for convergents. Write $[x_0, x_1, \ldots, x_n] = \dfrac{p_n}{q_n}$.

(a) Prove that

$$\begin{aligned} p_k &= x_k p_{k-1} + p_{k-2}, \\ q_k &= x_k q_{k-1} + q_{k-2}. \end{aligned}$$

(b) Prove that

$$[x_0, x_1, \ldots, x_{n-1}, x_n + 1/b] = \frac{bp_{n-1} + p_n}{q_n + q_{n-1}b}.$$

Exercise 1.9.23. Define a sequence by $x_{n+1} := 1 + 1/x_n$ starting at $x_0 = 1$. Prove that $\{x_n\}$ is a Cauchy sequence. Show that this provides the representation

$$\frac{\sqrt{5}+1}{2} = 1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cdots}}}. \tag{1.9.8}$$

This is the continued fraction representation of the **golden ratio** $\varphi = \frac{1}{2}(\sqrt{5}+1)$; that is,

$$\varphi = [1; 1, 1, 1, 1, 1, 1, \ldots]. \tag{1.9.9}$$

This number will reappear in Chapter 3 and the book by M. Livio [**202**] is dedicated to it.

Exercise 1.9.24. This exercise outlines a proof of the fact that the golden ratio φ is irrational. It appeared in J. Shallit and D. Ross [**270**]. Assume $\varphi = p/q$, with $\gcd(p, q) = 1$. Use the equation for φ to conclude that $p(p-q) = q^2$. Conclude that $p = 1$. Also $p^2 = q(p+q)$ implies that q divides p^2, so $q = 1$. It follows that $\varphi = 1$. This is a contradiction. Check the details.

Exercise 1.9.25. Z. Yachas [**315**] has produced a great proof that φ is irrational. The paper is quoted here: “For any pair of positive integers (p, q) such that $\varphi = p/q$, where φ is the positive root of $\varphi = 1 + 1/\varphi$, there is yet another pair $(q, p-q)$ with the same property, and whose sum is smaller. Since $\varphi \neq 2/1$, there can't be such a pair.” Check the details.

Definition 1.9.26. A continued fraction

$$x = [a_1,\, a_2,\, a_3,\, \ldots] \tag{1.9.10}$$

is called **periodic** if the sequence of integers $\{a_k : k \geq k_0\}$ is periodic, for some index k_0. That is, for some $t \in \mathbb{N}$, the identity $a_{j+nt} = a_j$ holds for $j \geq k_0$ and $n \in \mathbb{N}$. The smallest such t is called the **period** of the continued fraction.

The analog of Theorem 1.8.6 for continued fractions is stated below. See the text [**160**] for a proof.

Theorem 1.9.27. *A continued fraction is periodic if and only if x is the root of a quadratic polynomial with integer coefficients.*

Example 1.9.28. The continued fraction of $x = \sqrt{2}$ is

$$x = [\,1,\, 2,\, 2,\, 2,\, 2,\, 2, \ldots]$$

with period 1, and for $x = \sqrt{47}$

$$x = [\,6,\, 1,\, 5,\, 1,\, 12,\, 1,\, 5,\, 1,\, 12,\, 1,\, 5,\, 1,\, 12,\, 1,\, 5,\, 1,\, 12, \ldots]$$

with period 4.

Note 1.9.29. The computation of the continued fraction of $\sqrt{3}$ leads to a nice proof of the irrationality of $\sqrt{3}$. The argument presented below appears in the text by Y. Hellegouarch [**163**]. Assume $\sqrt{3} = a_1/b_1$. Then $\sqrt{3} = 1 + (\sqrt{3} - 1)$ and the first step in the construction of the continued fraction of $\sqrt{3}$ is to compute

$$\frac{1}{\sqrt{3}-1} = \frac{\sqrt{3}+1}{2}.$$

This yields

$$\frac{\sqrt{3}+1}{2} = \frac{b_1}{a_1 - b_1},$$

which implies $\sqrt{3} = (3b_1 - a_1)/(a_1 - b_1)$. Define

$$a_2 = 3b_1 - a_1, \quad b_2 = a_1 - b_1.$$

An easy argument shows that $b_2 < b_1$ and $a_2 < a_1$. Iteration produces a sequence $\{a_n,\, b_n\}$ with $\sqrt{3} = a_n/b_n$ with numerators and denominators strictly decreasing. This is a contradiction.

Note 1.9.30. Let $\lambda(n)$ be the least integer m such that the continued fraction of $\sqrt{n}$ has period m. In N. Sloane's database OEIS, entry $A013646$ gives the values of $\lambda(n)$ beginning with

$$1, 2, 3, 41, 7, 13, 19, 58, 31, 106, 43, 61.$$

Figure 1.9.1 illustrates this function.

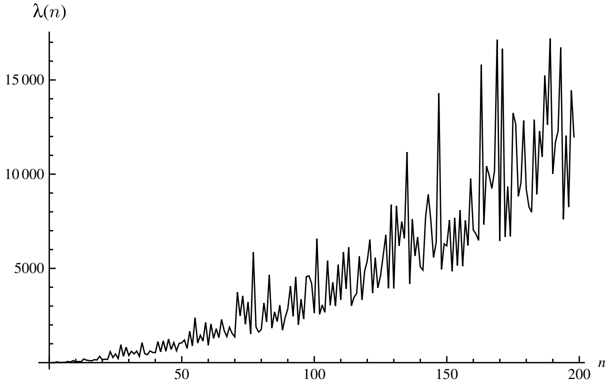


Figure 1.9.1. The function $\lambda(n)$.

Note 1.9.31. Given $x \in \mathbb{R}$, it is possible to construct a rational number that is arbitrarily close to x. The convergents p_n/q_n represent an example of such **rational approximations** to x. The error term satisfies

$$\left| x - \frac{p_n}{q_n} \right| < \frac{1}{2q_n^2}.$$

These approximations are optimal, in the following sense: let $n > 1$ and let $p/q \neq p_n/q_n$ be a rational number with denominator $q \leq q_n$. Then

$$\left| x - \frac{p}{q} \right| > \left| x - \frac{p_n}{q_n} \right|.$$

That is, among all rational numbers with denominators bounded by q_n, the convergents are **the best approximation** to x.

Note 1.9.32. In this text the real numbers have been introduced in different forms:

- **Cauchy sequences of rational numbers**. This is a Cauchy sequence $\{x_n\}$, with $x_n \in \mathbb{Q}$. This identifies the sequence $\{x_n\}$ with its limit $x \in \mathbb{R}$. An important goal is to have a constructive algorithm that gives x_n in terms of $\{x_1, \ldots, x_{n-1}\}$.
- **An expansion in base** b. Given $b \in \mathbb{N}$ and $x \in \mathbb{R}$, the base b-expansion of x is
$$x = \sum_{k=-n}^{\infty} \frac{x_k}{b^k}.$$
For a given x it is desirable to have an algorithm that gives x_k in terms of $\{x_{-n}, x_{-n+1}, \ldots, x_0, x_1, x_2, \ldots, x_{k-1}\}$.
- **A continued fraction expansion**. Every real number has a continued fraction of the form
$$x = x_0 + \cfrac{1}{x_1 + \cfrac{1}{x_2 + \cfrac{1}{x_3 + \cdots}}},$$
where $x_0 \in \mathbb{Z}$ and $x_i \in \mathbb{N}$ for $i > 0$. As in the previous two representations, it is desirable to have an algorithm that will determine x_k in terms of x.

Each of these forms present distinct aspects of the real numbers.

1.10. Fundamental sequences and completions

The procedure employed above to construct $\mathbb{R}$ from $\mathbb{Q}$ is employed very often in analysis. Given a set X and a **metric** on X, that is, a function $d : X \times X \to \mathbb{R}^+$ that allows us to state that two elements of X are close, it is possible to define the notion of Cauchy sequence in X. Then the **completion** of X is the set of Cauchy sequences (modulo some technical points: two sequences that differ by one converging to 0 must be identified).

A different type of metric on $\mathbb{Q}$ is described next.

1.10.1. The p-adic norm on $\mathbb{Q}$.

The goal of this part is to state a theorem of Ostrowski characterizing all (multiplicative) completions of $\mathbb{Q}$. Let p be a prime. Recall the notion of p-adic valuation defined in Subsection 1.7.1. Write $x \in \mathbb{Q}$ in the form

$$x = p^m \times \frac{b}{c}$$

where b, $c \in \mathbb{Z}$ are not divisible by p. Then $m \in \mathbb{Z}$ is the p-adic valuation of x, denoted by $\nu_p(x)$.

Definition 1.10.1. The **p-adic norm** of x is defined by

$$|x|_p := p^{-\nu_p(x)} \quad \text{if } x \neq 0 \text{ and } |0|_p := 0. \tag{1.10.1}$$

Observe that for a, $b \in \mathbb{N}$ the statement $a \equiv b \bmod p^m$ is equivalent to $|a-b|_p \leq p^{-m}$. Therefore, a number is *small* in the p-adic norm precisely when it is divisible by a large power of p. The reader will find in the texts by F. Gouvea [**142**] and M. R. Murty [**230**] a wonderful introduction to these ideas.

Exercise 1.10.2. Check that the p-adic norm satisfies

$$|x|_p = 0 \leftrightarrow x = 0, \; |xy|_p = |x|_p \, |y|_p, \quad \text{and} \; |x+y|_p \leq \text{Max}\left\{|x|_p, |y|_p\right\}.$$

Observe that this last property is stronger than the **triangle inequality**, $|x+y| \leq |x| + |y|$, for the usual absolute value in $\mathbb{Q}$.

Exercise 1.10.3. Prove that $\{1, p, p^2, p^3, \ldots\}$ is a Cauchy sequence in the p-adic norm.

Definition 1.10.4. The **field of p-adic numbers**, denoted by $\mathbb{Q}_p$, is the completion of $\mathbb{Q}$ under the p-adic norm.

Norms on fields. A **norm** on a field F is a function $v : F \to \mathbb{R}^+ \cup \{0\}$ such that

(1) $v(x) = 0$ if and only if $x = 0$,

(2) $v(x \cdot y) = v(x) \cdot v(y)$,

(3) $v(x+y) \leq v(x) + v(y)$.

Exercise 1.10.5. Two norms are said to be **equivalent** if they have the same convergent sequences. Prove that if p and q are different primes, then the p-adic and q-adic norms are not equivalent.

The last result in this chapter is a theorem of **Ostrowski** that characterizes all possible norms on $\mathbb{Q}$. In particular, this result describes all completions of $\mathbb{Q}$ that are compatible with its arithmetic structure.

Theorem 1.10.6. *Every norm on $\mathbb{Q}$ is a power of the usual absolute value or a power of the p-adic norm.*

1.11. Complex numbers

The last element of the chain (1.9.1) considered here is the set of **complex numbers** $\mathbb{C}$. This will give

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}.$$

The field of p-adic numbers does not form part of this chain.

The complex numbers were originally introduced by N. Tartaglia and G. Cardano in 1545 to address the so-called **casus irreducibilis**. This corresponds to a phenomenon that appears in the solution of a cubic equation: there are some situations in which, even though the three roots are real numbers, to find an algebraic expression for them requires an intermediate step that employs complex numbers. The solution of the cubic equation is described in Section 4.6.

The letter i is commonly employed to denote one of the two solutions of

$$x^2 + 1 = 0. \tag{1.11.1}$$

Naturally the second one must be $-i$. The set of complex numbers is defined by

$$\mathbb{C} = \left\{ a + ib : \; a, \, b \in \mathbb{R} \text{ and } i^2 = -1 \right\} \tag{1.11.2}$$

and it is provided with an arithmetic structure in a natural manner:

$$\begin{aligned} (a+ib) + (c+id) &= (a+c) + i(b+d), \\ (a+ib) \times (c+id) &= (ac-bd) + i(ad+bc). \end{aligned}$$

The rule for multiplication simply follows by distributing terms and employing $i^2 = -1$.

The next theorem states that, in some sense, the complex numbers represent the end of the chain of number systems described in this chapter. Each step on the chain has been produced from the previous one by adjoining solutions of polynomial equations, as in the case from $\mathbb{Z}$ to $\mathbb{Q}$, or by adjoining limits of Cauchy sequences, as in the passage from $\mathbb{Q}$ to $\mathbb{R}$ or $\mathbb{Q}_p$.

Theorem 1.11.1. *The complex numbers* $\mathbb{C}$ *are a complete, algebraically closed field. That is, every Cauchy sequence of elements in* $\mathbb{C}$ *converges to an element in* $\mathbb{C}$ ***and*** *every polynomial equation with complex coefficients has all its roots in* $\mathbb{C}$*.*

This is established in Section 4.5.

Chapter 2

Factorials and Binomial Coefficients

This chapter discusses the **factorial** $n!$ and **binomial coefficients** $\binom{n}{k}$ from several points of view. Special emphasis is placed on the arithmetic properties and is given to the question of extending them to functions of a real variable.

2.1. The definitions

The sum of the first n natural numbers

$$1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2} \tag{2.1.1}$$

was the example used in Chapter 1 to motivate the question of closed-form evaluation of finite sums by a function in a given class. The analog of (2.1.1) with products instead of sums is considered next.

Definition 2.1.1. Let $n \in \mathbb{N}$. The **factorial** of n is defined by

$$n! = 1 \cdot 2 \cdot 3 \cdots (n-1) \cdot n. \tag{2.1.2}$$

The first few values are $1! = 1$, $2! = 2$, $3! = 6$, $4! = 24$, $5! = 120$. The value of $n!$ grows very fast, for instance

$$40! = 815915283247897734345611269596115894272000000000.$$

Factorials can be defined inductively by

$$\begin{aligned} 1! &:= 1, \\ n! &:= n \times (n-1)!. \end{aligned} \tag{2.1.3}$$

This definition is extended to

$$0! = 1 \tag{2.1.4}$$

in order to be consistent with (2.1.3).

Note 2.1.2. The question of the existence of a fixed function f defined over $\mathbb{R}$ such that $f(n) = n!$ for $n \in \mathbb{N}$ is considered. This function would be the multiplicative analog of $\frac{1}{2}x(x+1)$ in (2.1.1). Euler's remarkable insight gave us the **gamma function**, defined by

$$\Gamma(z) = \int_0^\infty e^{-t}t^{z-1}\,dt. \tag{2.1.5}$$

It turns out that $f(x) = \Gamma(x+1)$ extends the factorials for real parameters and, in some sense, it is the unique reasonable extension. Special values include the remarkable identity

$$\left(\frac{1}{2}\right)! = \frac{\sqrt{\pi}}{2}. \tag{2.1.6}$$

This is explained in Chapter 16.

Note 2.1.3. The factorials have appeared in Theorem 1.3.3 in a combinatorial setting: they count the number of permutations of n objects.

Definition 2.1.4. Let $n \in \mathbb{N}$. The **binomial coefficients** are defined by

$$\binom{n}{k} = \frac{n!}{k!\,(n-k)!}, \tag{2.1.7}$$

for $0 \leq k \leq n$. For $n \in \mathbb{N}$, the binomial coefficients are defined as 0 if k is outside the range $0 \leq k \leq n$.

Exercise 2.1.5. Show that

$$\binom{n}{k} = \frac{1}{k!}n(n-1)(n-2)\cdots(n-k+1). \tag{2.1.8}$$

Introduce the **Pochhammer symbol**

$$(x)_k = x(x+1)(x+2)\cdots(x+k-1) \tag{2.1.9}$$

to write (2.1.8) as

$$\binom{n}{k} = \frac{(n-k+1)_k}{k!} = \frac{(-1)^k(-n)_k}{k!}. \tag{2.1.10}$$

The value

$$\binom{n}{0} = 1 \tag{2.1.11}$$

follows directly from Definition 2.1.4. The next result shows that the binomial coefficients are integers.

Theorem 2.1.6. *The binomial coefficients satisfy the recurrence*

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}. \tag{2.1.12}$$

In particular, $\binom{n}{k}$ is a natural number.

Proof. A direct calculation gives

$$\begin{aligned}\binom{n-1}{k} + \binom{n-1}{k-1} &= \frac{(n-1)!}{k!\,(n-1-k)!} + \frac{(n-1)!}{(k-1)!\,(n-k)!} \\ &= \frac{(n-1)!}{k!\,(n-k)!}\,(n-k+k) \\ &= \frac{n!}{k!\,(n-k)!},\end{aligned}$$

as claimed. □

Corollary 2.1.7. *Let $k \in \mathbb{N}$. Then $k!$ divides the product of any k consecutive integers.*

Proof. The product is $n(n-1)(n-2)\cdots(n-k+1)$, that is, $n!/(n-k)!$. This is divisible by $k!$ since the quotient is $\binom{n}{k}$. □

Proposition 2.1.8. *The binomial coefficients are symmetric: for $0 \leq k \leq n$,*

$$\binom{n}{k} = \binom{n}{n-k} \tag{2.1.13}$$

for $0 \leq k \leq n$.

Proof. This follows directly from the definition given in (2.1.7). □

2.2. A counting argument

The binomial coefficients are now expressed as the solution to a simple counting question. A **combination** of n objects taken k at a time is a subset of size k of the n objects. Naturally, in a set, the order in which the elements appear is irrelevant. For example, if $n = 4$ and $k = 2$, the six combinations are

$$\{x_1, x_2\},\ \{x_1, x_3\},\ \{x_1, x_4\},\ \{x_2, x_3\},\ \{x_2, x_4\},\ \{x_3, x_4\}.$$

The fact that $6 = \binom{4}{2}$ is a special case of the next theorem.

Theorem 2.2.1. *The number of combinations of n objects taken k at a time is $\binom{n}{k}$.*

Proof. There are n choices for the first object, $n-1$ for the second one, until $n-k+1$ for the kth one. The multiplicative principle gives a total of

$$n(n-1)\cdots(n-k+1) = \frac{n!}{(n-k)!} \tag{2.2.1}$$

choices. But each selection of k objects is counted $k!$ ways according to the number of permutations of these objects. Thus, the number of ways to pick k objects is

$$\frac{1}{k!} \times \frac{n!}{(n-k)!} = \binom{n}{k}. \tag{2.2.2}$$

□

Note 2.2.2. This interpretation provides a combinatorial proof that $\binom{n}{k}$ is a positive integer and also a second proof of Theorem 2.1.6.

Corollary 2.2.3. *The number of subsets of $\{1,\ 2,\ \ldots,\ n\}$ consisting of k elements is given by $\binom{n}{k}$.*

Proof. Divide the subsets of $\{1,\ 2,\ \ldots, n\}$ into two types: those that contain n and those that do not. Now count the $\binom{n}{k}$ subsets with k elements. Any set of the first type can be expressed as $A \cup \{n\}$ with $A \subset \{1,\ 2, \ldots, n-1\}$ and $|A| = k-1$. There are $\binom{n-1}{k-1}$ of this type. A set of the second type is automatically a subset of $\{1, 2, \ldots, n-1\}$. Therefore there are $\binom{n-1}{k}$ sets of the second type. The addition principle gives the relation

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}. \tag{2.2.3}$$

A combinatorial proof of Proposition 2.1.8 is presented next.

Proof. For every choice of k elements from a box with n elements, there is a corresponding choice of $n-k$ of elements, namely those you left in the box. □

Exercise 2.2.4. Consider paths on the lattice $\mathbb{Z} \times \mathbb{Z}$ starting at the origin $(0,0)$ and ending at (m,n) with steps of the form $N : (i,j) \mapsto (i,j+1)$, or $E : (i,j) \mapsto (i+1,j)$. Prove that the number of such paths is $\binom{m+n}{n}$.

2.3. The generating function of binomial coefficients

Given a sequence $\{a_n\}$, it is often convenient to introduce the **formal power series**

$$A(x) = \sum_{n=0}^{\infty} a_n x^n. \tag{2.3.1}$$

This is the **generating function** of the sequence $\{a_n\}$. There are cases in which this generating function can be given a concrete analytic expression. For instance, if $a_n \equiv 1$, then

$$A(x) = \sum_{n=0}^{\infty} x^n = \frac{1}{1-x}. \tag{2.3.2}$$

The classical **binomial theorem** provides an analytic expression for the generating function of the binomial coefficients.

Theorem 2.3.1. *The generating function of the binomial coefficients is*

$$\sum_{k=0}^{n} \binom{n}{k} x^k = (1+x)^n. \tag{2.3.3}$$

This can be scaled to

$$\sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k = (a+b)^n. \tag{2.3.4}$$

Proof. Define

$$BI_n(x) = \sum_{k=0}^{n} \binom{n}{k} x^k. \tag{2.3.5}$$

To produce a recurrence for $BI_n(x)$, multiply the recurrence for the binomial coefficients given in Theorem 2.1.6 by x^k and sum from $k=0$ to $k=n$. Recall that the binomial coefficients $\binom{n}{k}$ vanishes if $k<0$ or $k>n$. This gives

$$\begin{aligned} BI_n(x) = \sum_{k=0}^{n} \binom{n}{k} x^k &= \sum_{k=0}^{n} \binom{n-1}{k-1} x^k + \sum_{k=0}^{n} \binom{n-1}{k} x^k \\ &= \sum_{k=1}^{n} \binom{n-1}{k-1} x^k + \sum_{k=0}^{n-1} \binom{n-1}{k} x^k \\ &= \sum_{k=0}^{n-1} \binom{n-1}{k} x^{k+1} + \sum_{k=0}^{n-1} \binom{n-1}{k} x^k \\ &= BI_{n-1}(x) + xBI_{n-1}(x). \end{aligned}$$

It follows that

$$BI_n(x) = (1+x)BI_{n-1}(x), \tag{2.3.6}$$

and the result follows by induction. □

Exercise 2.3.2. Use the generating function to prove the symmetry relation $\binom{n}{k} = \binom{n}{n-k}$.

2.3.1. A combinatorial proof of the binomial theorem.

The binomial theorem

$$\sum_{k=0}^{n} \binom{n}{k} x^k = (1+x)^n \tag{2.3.7}$$

is now given a combinatorial proof. First note that both sides of (2.3.7) are polynomials of degree n. Hence it is enough to prove that (2.3.7) holds for $n+1$ distinct values of x. This result is a corollary of Exercise 4.4.4 that bounds the number of zeros of a polynomial by its degree. In particular, it is enough to show that it holds for values of $x \in \mathbb{N}$.

Suppose that x is a positive integer, and let A be the set of all functions $f : \{1, 2, \dots, n\} \longrightarrow \{1, 2, \dots, x+1\}$. Then the cardinality of A is $|A| = (1+x)^n$. Now count the elements of A in a different way. For $0 \leq k \leq n$, let A_k be the set of functions where exactly $n-k$ elements are mapped to the number $x+1$; that is,

$$A_k = \left\{ f \in A : \left| f^{-1}(x+1) \right| = n - k \right\}. \tag{2.3.8}$$

Then $A = \bigcup\limits_{k=0}^{n} A_k$, and the union is disjoint, so $|A| = \sum\limits_{k=0}^{n} |A_k|$.
To count the elements of A_k, choose a set Y of k elements of $\{1, 2, \dots, n\}$ in $\binom{n}{k}$ ways. There are x^k functions $Y \longrightarrow \{1, 2, \dots, x\}$, and each such function gives an element of A_k, by defining $f(i) = x+1$ for $i \in \{1, 2, \dots, n\} \setminus Y$. Hence $|A_k| = \binom{n}{k} x^k$, and (2.3.7) is proved.

This argument is typical of many combinatorial proofs of an identity where one of the sides is given by a finite sum. The strategy is to find a set whose cardinality is the other side of the identity and then try to partition the set in such a way that the terms of the sum are the cardinality of the sets in the partition. This is often done by finding a combinatorial interpretation for the index in the sum. In our case the index k is the number of elements that do not map to $x+1$.

2.4. An extension of the binomial theorem to noninteger exponents

The binomial theorem

$$(1+x)^n = \sum_{k=0}^{n} \binom{n}{k} x^k \tag{2.4.1}$$

has two components where $n \in \mathbb{N}$ plays a role. The goal in this section is to extend (2.4.1) to $n \in \mathbb{R}$. The first appearance of n is as the upper limit in the sum. This can be avoided by observing that the sum in (2.4.1) can be extended beyond n because $\binom{n}{k} = 0$ when $k > n$. This is consistent with the combinatorial interpretation of the binomial coefficients. The second appearance of $n \in \mathbb{N}$ is in the term $\binom{n}{k}$. This is extended by using (2.2.1) and writing

$$\binom{n}{k} = \frac{n(n-1)(n-2)\cdots(n-k+1)}{k!}, \tag{2.4.2}$$

and now the right-hand side makes sense for $n \notin \mathbb{N}$.

The notation is simplified by using the Pochhammer symbol defined in (2.1.9) to rewrite (2.4.1) as

$$(1+x)^n = \sum_{k=0}^{\infty} \frac{(n-k+1)_k}{k!} x^k. \tag{2.4.3}$$

Aside from the convergence issue, the right-hand side is well-defined for $n \in \mathbb{R}$.

The formalization of the above procedure is based on Taylor's theorem for the expansion of an analytic function applied to $f(x) = (1+x)^n$.

Theorem 2.4.1 (Taylor's theorem). *Let $n \geq 0$ and suppose that f is $(n+1)$-times differentiable on (a,b), with $f^{(n+1)}$ continuous on (a,b). Suppose that $f^{(n+1)}$ is integrable over (a,b), and fix $a < c < b$. Then,*

$$f(x) = \sum_{k=0}^{n} \frac{f^{(k)}(c)}{k!}(x-c)^k + \frac{h_{n+1}(x)}{(n+1)!}(x-c)^{n+1}, \tag{2.4.4}$$

where the remainder has the representation

$$h_{n+1}(x) = (n+1)\int_0^1 (1-s)^n f^{(n+1)}[c+s(x-c)]\,ds. \tag{2.4.5}$$

The reader will find a proof of this result in the textbook by O. Hijab [**168**]. Assume that for $x \in I \subset \mathbb{R}$ the remainder converges to 0 as $n \to \infty$. Then

$$f(x) = \sum_{k=0}^{\infty} \frac{f^{(k)}(c)}{k!}(x-c)^k \tag{2.4.6}$$

for $x \in I$.

Theorem 2.4.2. *Let $a \in \mathbb{R}$ and $|x| < 1$. Then the binomial theorem states that*

$$(1-x)^{-a} = \sum_{k=0}^{\infty} \frac{(a)_k}{k!} x^k. \tag{2.4.7}$$

Proof. The function $f(x) = (1-x)^{-a}$ satisfies

$$f^{(k)}(x) = (a)_k (1-x)^{-a-k}.$$

The expansion (2.4.7) now follows from Theorem 2.4.1 and the next exercise. □

Exercise 2.4.3. Prove that in the case $f(x) = (1-x)^{-a}$, the error term $h_{n+1}(x)$ in Theorem 2.4.1 converges to 0.

Exercise 2.4.4. Use Theorem 2.4.2 to obtain an expansion for $f(x) = 1/\sqrt{1-4x}$. The answer will provide an analytic expression for the **central binomial coefficients** $\binom{2n}{n}$.

Note 2.4.5. This note contains the approximations to square roots promised in Subsection 1.9.4. The reader will find the basic properties of power series in Theorem 11.1.4. In particular it follows that the series (2.4.7) converges for $-1 < x < 1$. The special values $a = \frac{1}{2}$ and $x = \frac{1}{2}$ yield the expression

$$\sum_{k=0}^{\infty} \left(\frac{1}{2}\right)_k \frac{1}{2^k\, k!} = \sqrt{2}. \tag{2.4.8}$$

The sequence of rational numbers

$$a_n = \sum_{k=0}^{n} \left(\frac{1}{2}\right)_k \frac{1}{2^k\, k!} = \sum_{k=0}^{n} 2^{-3k} \binom{2k}{k} \tag{2.4.9}$$

converges to $\sqrt{2}$. The reader can check that a_{10} gives three correct digits for $\sqrt{2}$.

The continued fraction of $\sqrt{2}$ is given by

$$\sqrt{2} = [1,\ 2,\ 2,\ \ 2,\ 2, \ldots]\,. \tag{2.4.10}$$

It is interesting to compare this with the (finite) continued fraction of a_n. For example,

$$a_{10} = \frac{379582629}{268435456} = [1,2,2,2,2,4,8,2,9,3,1,1,8,3,1,2,5,1,2]\,.$$

Define b_n to be the first entry in the continued fraction of a_n, after the first one, that is different than 2. For example, $b_{10} = 6$. The sequence $\{b_n : n \in \mathbb{N}\}$ begins with

$$\{2,\, 3,\, 3,\, 3,\, 4,\, 4,\, 5,\, 5,\, 6,\, 6,\, 6,\, 7,\, 7,\, 8,\, 8,\, 9,\, 9,\, 9,\, 10,\, 10\}\,.$$

The length of the blocks seems to have a more regular pattern. It starts as

$$\{1,\, 3,\, 2,\, 2,\, 3,\, 2,\, 2,\, 3,\, 2,\, 3,\, 2,\, 3,\, 2,\, 3,\, 2,\, 3\}\,.$$

The pattern $\{3,\, 2\}$ is interrupted by repeating blocks starting at positions

$$\{3,\, 6,\, 36,\, 53,\, 70,\, 85,\, 98,\, 113,\, 126,\, 139,\, 152,\, 165,\, 178,\, 191\}.$$

What does this mean?

Exercise 2.4.6. Compile data for other radicals and provide an explanation.

2.5. Congruences for factorials and binomial coefficients

In this section a variety of congruences satisfied by factorials and binomial coefficients is considered.

2.5.1. Congruences for factorials. The first result reported here is due to J. Wilson and it characterizes primes in terms of a congruence. The result was announced by Wilson's advisor E. Waring in [**305**]. The proof of this result employs the next two exercises.

Exercise 2.5.1. Prove that if p is prime and $0 < a < p - 1$, then the congruence $ax \equiv b \bmod p$ has a unique solution in the interval $0 \leq x < p$. In particular every such a has a unique multiplicative inverse modulo p. **Hint:** The greatest common divisor of a and p is 1.

Exercise 2.5.2. Prove that if p is prime, then 1 and $p - 1$ are the only numbers that are their own multiplicative inverses.

Theorem 2.5.3. *Let $n \in \mathbb{N}$. Then*

$$(n-1)! \equiv \begin{cases} -1 \bmod n & \textit{if } n \textit{ is prime}, \\ 0 \bmod n & \textit{if } n \textit{ is not prime}. \end{cases} \tag{2.5.1}$$

Proof. In the product

$$(p-1)! = (p-1) \times (p-2) \times \cdots \times 2 \times 1 \tag{2.5.2}$$

pair each integer with its unique inverse. Exercise 2.5.2 shows that

$$(p-1)! \equiv (p-1) \times 1 \equiv -1. \tag{2.5.3}$$

The case of n not prime is left as Exercise 2.5.4. □

Exercise 2.5.4. Check that $(n-1)! \equiv 0 \bmod n$ if n is not prime.

Exercise 2.5.5. Discuss this as a method to determine the primality of $n \in \mathbb{N}$. In particular, count the number of operations required to accomplish this task.

A second proof of Wilson's theorem, Theorem 2.5.3, is presented now. It is based on an identity of two polynomials over $\mathbb{Z}_p$. This is established by showing that their values match at more places than the common degree.

Proposition 2.5.6. *Let p be prime. Then*

$$x^{p-1} - 1 \equiv (x-1)(x-2)\cdots(x-p+1) \mod p.$$

Proof. The polynomial

$$T_p(x) = x^{p-1} - 1 - (x-1)(x-2)\cdots(x-p+1) \tag{2.5.4}$$

is of degree $p-2$ (the coefficient of x^{p-1} vanishes). Fermat's little theorem, established in Subsection 2.5.2, shows that $T_p(x)$ vanishes at the $p-1$ nonzero elements of $\mathbb{Z}_p$. Proposition 4.4.1 shows that it must vanish identically. This gives the identity. □

Proof of Wilson's theorem. The vanishing of the constant term in $T_p(x)$ in (2.5.4) gives the result.

The extension of Wilson's theorem given in the next exercise was proposed by R. S. Luthar and W. C. Waterhouse in [**206**].

Exercise 2.5.7. Let $p \geq n$ be prime. Prove that

$$(n-1)!\,(p-n)! \equiv (-1)^n \mod p.$$

Hint: Use $(-1)k \equiv p-k$ for $1 \leq k \leq n$.

Note 2.5.8. The coefficients of a polynomial

$$P(x) = (x - a_1)(x - a_2) \cdots (x - a_n) = \sum_{j=0}^{n} (-1)^j s_j(a_1, a_2, \ldots, a_n) x^j$$

are given in terms of the **symmetric functions**

$$s_j(a_1,\, a_2, \ldots, a_n) = \sum_{i_1 < i_2 < \cdots < i_j} \prod_{r=1}^{j} a_{i_r}. \tag{2.5.5}$$

For example,

$$\begin{aligned} s_1(a_1,\, a_2, \ldots, a_n) &= a_1 + a_2 + \cdots + a_n, \\ s_2(a_1,\, a_2, \ldots, a_n) &= a_1a_2 + a_1a_3 + \cdots + a_{n-1}a_n, \end{aligned}$$

and

$$s_n(a_1,\, a_2, \ldots, a_n) = a_1a_2 \cdots a_n.$$

Proposition 2.5.6 shows that for p prime and $1 \leq j \leq p-2$, the symmetric functions of $\{1,\, 2,\, \ldots, , p-1\}$ satisfy

$$s_j(1, 2, \ldots, p-1) \equiv 0 \bmod p. \tag{2.5.6}$$

2.5.2. Fermat's little theorem. The binomial theorem provides a direct proof of a congruence known as **Fermat's little theorem**. The proof begins with an exercise.

Exercise 2.5.9. Let p be a prime and let $1 \leq k \leq p-1$. Prove that p divides $\binom{p}{k}$. **Hint:** Use the identity

$$k\binom{p}{k} = (p-k+1)\binom{p}{k-1}, \qquad \text{for } 1 \leq k \leq p.$$

Corollary 2.5.10. *For p prime,*

$$(a+b)^p \equiv a^p + b^p \bmod p. \tag{2.5.7}$$

Theorem 2.5.11. *Let $a \in \mathbb{N}$ and let p be a prime. Then $a^p \equiv a \bmod p$.*

Proof. The identity above, with $b = 1$, yields

$$(a+1)^p \equiv a^p + 1 \bmod p. \tag{2.5.8}$$

This proves the result by induction on a, starting at $a = 0$. □

Note 2.5.12. Fermat's little theorem shows that if $a \in \mathbb{N}$ is not divisible by p, the number

$$q_a(p) := \frac{a^{p-1}-1}{p} \tag{2.5.9}$$

is an integer, called the **Fermat quotient of base** a. These numbers are related to Fermat's last theorem (FLT). This is the (famous) conjecture by Fermat that the equation $x^n + y^n = z^n$ has only trivial solutions for $n \geq 3$. The trivial solutions are those for which one of the unknowns vanishes. The solution of this conjecture was given by A. J. Wiles [**312**]. The first case of FLT for the prime p is the statement that $x^p + y^p = z^p$ has no solutions in nonzero integers x, y, z not multiples of p. Wieferich proved that if the first case of FLT is false, then $q_2(p)$ must be divisible by p. The only known primes that satisfy this condition are $p = 1093$ and $p = 3511$. (The book by P. Ribenboim [**251**] contains details.) A nice presentation of the background required for this topic is given in the book by Y. Hellegouarch [**163**].

2.5.3. Congruences for binomial coefficients.

The literature contains a variety of congruences for binomial coefficients. The first example is a beautiful congruence for general binomial coefficients due to E. Lucas.

Exercise 2.5.13. Let n, $m \in \mathbb{N}$ and let p be a prime. Then

$$\binom{n}{m} \equiv \binom{\lfloor n/p \rfloor}{\lfloor m/p \rfloor} \binom{n \bmod p}{m \bmod p} \bmod p. \tag{2.5.10}$$

Lucas' theorem is stated next.

Theorem 2.5.14. *Let p be a prime. Assume $a = a_0 + a_1 p + \cdots + a_k p^k$ and $b = b_0 + b_1 p + \cdots + b_k p^k$ are the representation of a, b in base p. Then*

$$\binom{a}{b} \equiv \binom{a_0}{b_0}\binom{a_1}{b_1} \cdots \binom{a_k}{b_k} \bmod p.$$

Proof. The term $\binom{a}{b}$ is the coefficient of x^b in $(1+x)^a$. Then

$$\begin{aligned}
(1+x)^a &= (1+x)^{a_0+a_1p+\cdots+a_kp^k} \\
&= \prod_{i=0}^{k}(1+x)^{a_ip^i} \\
&\equiv \prod_{i=0}^{k}(1+x^{p^i})^{a_i} \\
&= \prod_{i=0}^{k}\sum_{j_i=0}^{p-1}\binom{a_i}{j_i}x^{j_ip^i} \\
&= \sum_{j_0,j_1,\cdots,j_k=0}^{p-1}\left[\prod_{i=0}^{k}\binom{a_i}{j_i}\right]x^{j_0+j_1p+\ldots+j_kp^k} \bmod p.
\end{aligned}$$

The claim now follows from the uniqueness of base p expansions. □

The remainder of the section presents congruences for the central binomial coefficients $\binom{2p}{p}$. The main goal is to provide details of a congruence discovered by J. Wolstenholme [**314**] for the residue of $\binom{2p}{p}$ modulo p^3. The discussion begins with some elementary remarks.

It has been established that

$$\binom{p}{k} \equiv 0 \bmod p$$

for $1 \leq k \leq p-1$.

Exercise 2.5.15. Check that for p prime and $1 \leq k \leq p-1$, the congruence

$$\binom{p}{k} \not\equiv 0 \bmod p^2 \tag{2.5.11}$$

holds. Conclude that, for $1 \leq k \leq p-1$,

$$\nu_p\binom{p}{k} = 1. \tag{2.5.12}$$

The basic identity

$$\sum_{k=0}^{n}\binom{n}{k}^2 = \binom{2n}{n} \tag{2.5.13}$$

is now used to establish divisibility properties of the central binomial coefficient. This identity will be considered in Chapter 5.

Proposition 2.5.16. *For p prime, it follows that*

$$\binom{2p}{p} \equiv 2 \bmod p. \tag{2.5.14}$$

This is extended to mod p^2 *in Theorem* 2.5.18 *and to* mod p^3 *in Theorem* 2.5.21*.*

Proof. The result follows from the identity

$$\binom{2p}{p} = \sum_{k=0}^{p} \binom{p}{k}^2 \equiv 2 \bmod p. \tag{2.5.15}$$

□

Exercise 2.5.17. Prove that for p prime and $1 \leq k \leq p-2$, the congruence

$$\binom{p-2}{k-1} \equiv (-1)^{k-1} k \bmod p \tag{2.5.16}$$

holds. This is a problem proposed by P. L. Chessin [**100**].

The identity

$$\binom{2p}{p} = 2\binom{2p-1}{p-1} \tag{2.5.17}$$

and (2.5.14) show that

$$\binom{2p-1}{p-1} \equiv 1 \bmod p. \tag{2.5.18}$$

The next theorem, due to C. Babbage, extends this result. In particular, the proof shows a relation between this question and harmonic numbers treated in Section 11.11.

Theorem 2.5.18. *Let p be an odd prime. Then*

$$\binom{2p-1}{p-1} \equiv 1 \bmod p^2. \tag{2.5.19}$$

This implies

$$\binom{2p}{p} \equiv 2 \bmod p^2.$$

Proof. The binomial coefficient is

$$\binom{2p-1}{p-1} = \frac{(2p-1)(2p-2)\cdots(p+1)}{(p-1)!}.$$

Its numerator, written as

$$(x+p-1)(x+p-2)\cdots(x+2)(x+1) \text{ with } x = p,$$

is expanded in the form

$$x^{p-1} + s_{p-2}x^{p-2} + \cdots + s_2x^2 + s_1x + s_0.$$

The coefficient s_0 is $(p-1)!$ and s_1 is the sum of products of $p-2$ terms from $\{1, 2, \ldots, p-2, p-1\}$. This gives

$$\binom{2p-1}{p-1} = \frac{p^{p-1} + s_{p-2}p^{n-2} + \cdots + s_2p^2 + s_1p}{(p-1)!} + 1. \tag{2.5.20}$$

The result follows from the congruence $s_1 \equiv 0 \bmod p$, established in Proposition 2.5.6. A second proof of this congruence is presented next. Computing in $\mathbb{Z}_p$ the integers modulo p, the term s_1 is

$$s_1 = (p-1)!\sum_{j=1}^{p-1}\frac{1}{j}.$$

The set $\{1, 2, \ldots, p-1\}$ is the same as $\{1^{-1}, 2^{-1}, \ldots, (p-1)^{-1}\}$ modulo p and $(p-1)! \equiv -1 \bmod p$ by Wilson's theorem. It follows that

$$s_1 \equiv -\sum_{j=1}^{p-1} j = -\frac{p(p-1)}{2} \equiv 0 \bmod p.$$

□

Exercise 2.5.19. Give a one-line proof of the theorem using the identity (2.5.15). **Hint:** The terms divisible by p are squared.

The proof above shows a divisibility result for the **harmonic number**

$$H_{n-1} = 1 + \frac{1}{2} + \cdots + \frac{1}{n-1}.$$

These numbers are considered in Section 11.11.

Corollary 2.5.20. *The numerator of the harmonic number H_{p-1}, for p prime, is divisible by p.*

The congruence for the central binomial coefficient $\binom{2p}{p}$ was extended modulo p^3 by J. Wolstenholme [**314**].

Theorem 2.5.21. *Let $p \geq 5$ be a prime. Then*

$$\binom{2p-1}{p-1} = \frac{1}{2}\binom{2p}{p} \equiv 1 \bmod p^3.$$

The proof of the theorem will employ some expansions for the binomial coefficients. These are described first. The notation

$$H_{i,p-1} = \sum_{j=1}^{p-1} \frac{1}{j^i} \tag{2.5.21}$$

for the **generalized harmonic numbers** is employed.

Start with

$$\begin{aligned}\binom{n-1}{k} &= \frac{(n-1)(n-2)\cdots(n-k)}{1\cdot 2\cdots k} \\ &= (-1)^k \prod_{j=1}^{k}\left(1-\frac{n}{j}\right) \\ &= (-1)^k\left[1 - n\sum_{0<i<n}\frac{1}{i} + n^2\sum_{0<i<j<n}\frac{1}{ij} + \cdots + (-1)^k n^k \frac{1}{k!}\right].\end{aligned}$$

In terms of the elementary symmetric functions s_j this may also be expressed as

$$\binom{n-1}{k} = (-1)^k \sum_{j=0}^{k}(-1)^j n^j s_j\left(\frac{1}{1},\frac{1}{2},\ldots,\frac{1}{k}\right).$$

The elementary symmetric functions may be expressed in terms of power-sum symmetric polynomials

$$p_j(x_1, x_2, \ldots, x_k) = \sum_{i=1}^{k} x_i^j. \tag{2.5.22}$$

For example, $s_1 = p_1$ and $2s_2 = p_1^2 - p_2$. Now assume p is an odd prime and take $n = 2p$ and $k = p-1$ to obtain

$$\begin{aligned}\binom{2p-1}{p-1} &\equiv 1 - 2p\sum_{0<i<p}\frac{1}{i} + 4p^2\sum_{0<i<j<p}\frac{1}{ij} \bmod p^3 \\ &= 1 - 2pH_{1,p-1} + 2p^2H_{1,p-1}^2 - 2p^2H_{2,p-1} \bmod p^3.\end{aligned}$$

Now recall that $H_{1,p-1}$ is divisible by p ($H_{1,p-1}$ is the harmonic number H_{p-1}). The argument is based on the fact that if the index i runs over the nonzero residue classes modulo p, so does the inverse $1/i$. Therefore, the previous identity contains Babbage's congruence (2.5.19). Similarly,

$$H_{2,p-1} = \sum_{i=1}^{p-1} \frac{1}{i^2} \equiv \sum_{i=1}^{p-1} i^2 = \frac{1}{6}(p-1)(2p-1)p \equiv 0 \bmod p.$$

This reduces to

$$\binom{2p-1}{p-1} \equiv 1 - 2pH_{1,p-1} \bmod p^3. \tag{2.5.23}$$

Wolstenholme's theorem, Theorem 2.5.21, follows from $H_{1,p-1} \equiv 0 \bmod p^2$. To establish this congruence, observe that

$$\begin{aligned}\binom{2p-1}{p-1} &= \frac{(2p-1)(2p-2)\cdots(p+1)}{(p-1)(p-2)\cdots 1} \\ &= \prod_{k=1}^{p-1}\left(1+\frac{p}{k}\right) \\ &\equiv 1 + p\sum_{0<i<p}\frac{1}{i} + p^2 \sum_{0<i<j<p}\frac{1}{ij} \bmod p^3 \\ &= 1 + pH_{1,p-1} + \frac{1}{2}p^2H_{1,p-1}^2 - \frac{1}{2}p^2H_{2,p-1} \bmod p^3.\end{aligned}$$

This gives

$$\binom{2p-1}{p-1} \equiv 1 + pH_{1,p-1} \bmod p^3. \tag{2.5.24}$$

Then (2.5.23) and (2.5.24) imply that $3pH_{1,p-1}$ is divisible by p^3; thus $H_{1,p-1}$ is divisible by p^2. Wolstenholme's congruence now comes from (2.5.23).

Note 2.5.22. (1) Primes for which the congruence in Theorem 2.5.21 holds modulo p^4 are called **Wolstenholme primes**. R. J. McIntosh and E. L. Roettger report in [**212**] that $p = 16843$ and $p = 2124679$ are the only Wolstenholme primes up to 10^9. Infinitely many are conjectured to exist. It is also conjectured that there are no primes for which the congruence holds modulo p^5.

(2) It is conjectured that the converse of Wolstenholme's theorem, Theorem 2.5.21, is true. Namely, if $\binom{2n-1}{n-1} \equiv 1 \bmod n^3$, then n is prime. It has been verified up to $n < 10^9$.

(3) R. Tauraso [**288**] has established the congruence

$$\binom{2p-1}{p-1} \equiv 1 + 2p \sum_{i=1}^{p-1} \frac{1}{i} + \frac{2}{3} p^3 \sum_{i=1}^{p-1} \frac{1}{i^3} \bmod p^6.$$

(4) Wolstenholme's congruence can be generalized to

$$\binom{2p-1}{p-1} \equiv 1 - \frac{2}{3} p^3 B_{p-3} \bmod p^4$$

where B_{p-3} is the Bernoulli number. This shows that p is a Wolstenholme prime if and only if p divides the numerator of the Bernoulli number B_{p-3}. This divisibility property is related to Fermat's last theorem [**251**]. The reader will find properties of Bernoulli numbers in Chapter 13.

(5) The following statements are equivalent:

(a) p is a Wolstenholme prime.

(b) p divides the numerator of the Bernoulli number B_{p-3}.

(c) The congruence

$$\sum_{k=\lfloor p/6 \rfloor + 1}^{\lfloor p/4 \rfloor} \frac{1}{k^3} \equiv 0 \bmod p \tag{2.5.25}$$

holds.

(6) The next example contains information about the central binomial coefficients. Let $p > 2$ be a prime and write $p = 2q + 1$. Then

$$\binom{2q}{q} \equiv (-1)^q 2^{4q} \bmod p^3. \tag{2.5.26}$$

This was established by F. Morley [**224**]. It was improved by L. Carlitz [**91**] to

$$\binom{2q}{q} \equiv (-1)^q \left(2^{4q} + \tfrac{1}{12} p^3 B_{p-3} \right) \bmod p^4. \tag{2.5.27}$$

(7) I. Gessel [**135**] presents an extension of a result stated by M. Bayat [**42**]. Let m and k be positive integers and define

$$G(m,k) = \sum_{i \in R_m} \frac{1}{i^k},$$

where R_m is the set of integers from 1 to $m-1$ relatively prime to m. Then, if k is not a multiple of $p-1$ for any prime p dividing m, then $G(m,k) \equiv 0 \bmod m$. Also, if k is odd and $k+1$ is not a multiple of $p-1$ for any prime p dividing m, then $G(m,k) \equiv 0 \bmod m^2$.

2.6. The prime factorization of $n!$

This section describes the prime factorization of factorials. It is clear that only primes $p \leq n$ appear in this factorization. For example,

$$20! = 2^{18} \cdot 3^8 \cdot 5^4 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19.$$

The question is to determine the exact exponent of p that divides $n!$. Recall that $\nu_p(n)$, defined in Definition 1.7.1, is the exact exponent of p in the prime factorization of n. The factorization of 20! given above shows that $\nu_3(20!) = 8$ and $\nu_{23}(20!) = 0$. The first result is an analytic expression for $\nu_p(n!)$.

Theorem 2.6.1. *Let $n \in \mathbb{N}$ and let p be a prime. Then*

$$\nu_p(n!) = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor.$$

Proof. The product $n! = n \cdot (n-1) \cdot (n-2) \cdots 3 \cdot 2 \cdot 1$ has $\left\lfloor \frac{n}{p} \right\rfloor$ terms divisible by p. Take a factor of p out of each one them. The remaining product now has $\left\lfloor \frac{n}{p^2} \right\rfloor$ terms that are still divisible by p (those that were originally divisible by p^2). This process must end in a finite number of steps. □

Exercise 2.6.2. The sum (2.6.1) terminates after $\lfloor \log_p n \rfloor$ steps.

Exercise 2.6.3. Prove that

$$\nu_p(n) = \sum_{k=1}^{\infty} \left(\left\lfloor \frac{n}{p^k} \right\rfloor - \left\lfloor \frac{n-1}{p^k} \right\rfloor \right).$$

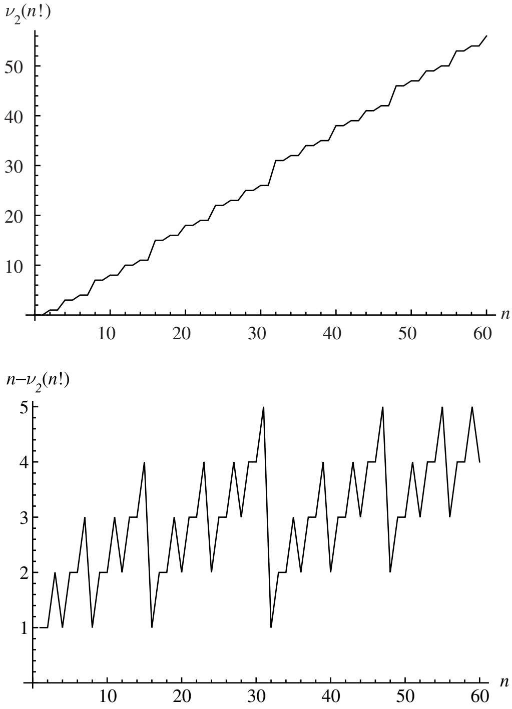


Figure 2.6.1. The valuation of $n!$ and the deviation from linear growth.

Moreover, check that the summand corresponding to the index k is a periodic function of n with period p^k.

Figure 2.6.1 shows the graph of $\nu_2(n!)$ and the difference $n - \nu_2(n!)$. The structure of the function $\nu_2(n!)$ seen in the figures, in particular its linear growth, is evident. An explicit expression for the error term $\nu_p(n!) \sim n/(p-1)$ was discovered by A. M. Legendre [**198**].

Theorem 2.6.4. *Let $n \in \mathbb{N}$, let p be a prime, and let*

$$n = a_0 + a_1 p + a_2 p^2 + \cdots + a_r p^r \tag{2.6.1}$$

be the expansion of n in base p. Then

$$\nu_p(n!) = \frac{n - s_p(n)}{p-1} \tag{2.6.2}$$

where $s_p(n) := a_0 + a_1 + \cdots + a_r$ *is the sum of base-*p *digits of* n*. In particular,*

$$\nu_2(n!) = n - s_2(n). \tag{2.6.3}$$

Proof. The summands in (2.6.1) are rewritten in terms of the digits of n as

$$\begin{array}{ccl} \left\lfloor \dfrac{n}{p} \right\rfloor & = & a_1 + a_2 p + \cdots + a_r p^{r-1}, \\ \left\lfloor \dfrac{n}{p^2} \right\rfloor & = & a_2 + a_3 p + \cdots + a_r p^{r-2}, \\ \cdots & \cdots & \cdots \\ \left\lfloor \dfrac{n}{p^r} \right\rfloor & = & a_r. \end{array}$$

Then

$$\nu_p(n!) = a_1 + a_2(1+p) + a_3(1+p+p^2) + \cdots + a_r(1+p+\cdots+p^{r-1}).$$

Multiplying by $1-p$ gives

$$(1-p)\nu_p(n!) = a_1(1-p) + a_2(1-p^2) + \cdots + a_r(1-p^r),$$

which yields the result. □

Exercise 2.6.5. Check that $|s_p(n)| \leq C \ln n$ for some constant C. Conclude that $\nu_p(n!) \sim n/(p-1)$ as $n \to \infty$.

Exercise 2.6.6. Discuss the behavior of $x^n/n!$ as $n \to \infty$ in the usual norm and in the p-adic norm defined in (1.10.1). The expression considered here is the general term of the exponential function discussed in Chapter 11.

The next result gives a result of Kummer for the p-adic valuation of binomial coefficient $\binom{n}{m}$.

Let $t = n - m$ and write n, m, and t in base p as in (2.6.1). Denote the digits of n by n_j and those of m, t by m_j, t_j, respectively. Now let $\varepsilon_j = 1$ if there is a **carry** in the jth digit when adding m and t in base p, and let $\varepsilon_j = 0$ otherwise.

Theorem 2.6.7. *The* p*-adic valuation of* $\binom{n}{m}$ *is given by*

$$\nu_p\left(\binom{n}{m}\right) = \sum_{j \geq 0} \varepsilon_j. \tag{2.6.4}$$

Proof. Observe that $n_0 = m_0 + t_0 - p\varepsilon_0$ and $n_j = m_j + t_j - p\varepsilon_j + \varepsilon_{j-1}$ for each $j \geq 1$. Legendre's formula states that

$$\begin{aligned}
\nu_p\left(\binom{n}{m}\right) &= \frac{s_p(m) + s_p(t) - s_p(n)}{p-1} \\
&= \sum_{j \geq 0} \frac{m_j + t_j - n_j}{p-1} \\
&= \frac{1}{p-1}\left(p\varepsilon_0 + \sum_{j \geq 1}(p\varepsilon_j - \varepsilon_{j-1})\right) \\
&= \sum_{j \geq 0} \varepsilon_j,
\end{aligned}$$

as claimed. □

Exercise 2.6.8. Prove that the power of p that divides $\binom{n}{m}$ is the number of integers $j \geq 0$ for which

$$\left\lfloor \frac{n}{p^j} \right\rfloor > \left\lfloor \frac{m}{p^j} \right\rfloor + \left\lfloor \frac{n-m}{p^j} \right\rfloor .$$

Hint: Study the values of the function

$$f(x, y, p) = \left\lfloor \frac{x}{p} \right\rfloor - \left\lfloor \frac{y}{p} \right\rfloor - \left\lfloor \frac{x-y}{p} \right\rfloor$$

for $y \leq x$.

Exercise 2.6.9. Prove that all entries in the nth row of Pascal's triangle are odd if and only if n has the form $2^r - 1$. Prove that this is exactly the case where there are no carries.

Exercise 2.6.10. In the notation of Theorem 2.6.4, write $n! = p^{\nu_p(n!)}m$ with m not divisible by p. Prove that

$$m \equiv (-1)^{\nu_p(n!)} a_r! \cdots a_1! a_0! \bmod p. \tag{2.6.5}$$

Use this result to create an algorithm that finds the last nonzero digit of $n!$. Use it to find the last nonzero digit of 1000000!.

Note 2.6.11. The p-adic valuation of n has a definite structure that will become useful in the study of p-adic valuations of more complicated functions. Figure 2.6.2 shows the 3-adic and 5-adic valuations of n.

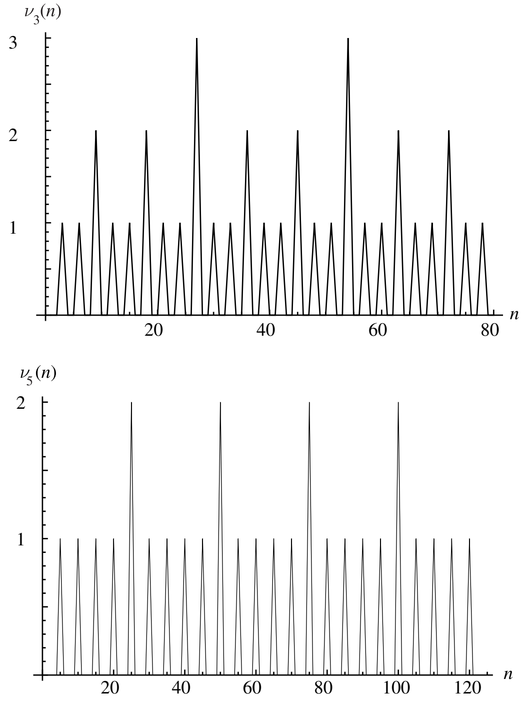


Figure 2.6.2. The 3-adic and 5-adic valuation of n.

2.6.1. Optimal bounds for $\nu_p(n!)$.

Optimal bounds for the p-adic valuation of $n!$ appeared in B. Berndt and S. Bhargava [**50**, page 593]. This is an expository paper about Ramanujan's work.

Theorem 2.6.12. *Let p be a prime. Then*

$$\frac{n}{p-1} - \frac{\ln(n+1)}{\ln p} \leq \nu_p(n!) \leq \frac{n-1}{p-1} \tag{2.6.6}$$

and both bounds are achieved for some special choice of n. In particular,

$$\lim_{n\to\infty} \frac{\nu_p(n!)}{n} \quad = \quad \frac{1}{p-1}. \tag{2.6.7}$$

Proof. If $n = p^r$, then

$$\begin{aligned}\nu_p(n!) &= \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \cdots + \left\lfloor \frac{n}{p^r} \right\rfloor \\ &= p^{r-1} + p^{r-2} + \cdots + p + 1 \\ &= \frac{p^r - 1}{p-1} = \frac{n-1}{p-1},\end{aligned}$$

so the upper bound is achieved.

If $n = p^{r+1} - 1$, then

$$\begin{aligned}\nu_p(n!) &= \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \cdots + \left\lfloor \frac{n}{p^r} \right\rfloor \\ &= (p^r - 1) + (p^{r-1} - 1) + \cdots + (p-1) \\ &= \frac{p^{r+1} - 1}{p-1} - (r+1) \\ &= \frac{n}{p-1} - \frac{\ln(n+1)}{\ln p},\end{aligned}$$

so the lower bound is achieved.

The first inequality is easy to establish: write

$$n = a_0 + a_1 p + a_2 p^2 + \cdots + a_r p^r \quad \text{with } 0 \leq a_j \leq p-1$$

and $a_r \neq 0$. Legendre's formula gives

$$\nu_p(n!) = \frac{n}{p-1} - \frac{1}{p-1} \sum_{j=0}^{r} a_j.$$

Therefore $\nu_p(n!) \leq (n-1)/(p-1)$. The second inequality is more difficult and the proof presented here is due to B. Reznick. Recall the function $s_p(n)$ defined in Theorem 2.6.4. It is required to prove

$$s_p(n) \leq (p-1) \frac{\ln(n+1)}{\ln p}.$$

Write $s_p(n) = k(p-1) + s$ with $0 \leq s \leq p-2$. Then

$$\begin{aligned} n &\geq (p-1)p^0 + (p-1)p + (p-1)p^2 + \cdots + (p-1)p^{k-1} + sp^k \\ &= (s+1)p^k - 1,\end{aligned}$$

and it follows that

$$\begin{aligned}(p-1)\frac{\ln(n+1)}{\ln p} &\geq (p-1)\frac{\ln((s+1)p^k)}{\ln p} \\ &= k(p-1)+(p-1)\frac{\ln(s+1)}{\ln p}.\end{aligned}$$

To complete the proof, it is required to show that

$$s \leq (p-1)\frac{\ln(s+1)}{\ln p}. \tag{2.6.8}$$

The inequality (2.6.8) holds for $s=0$, and for $s \geq 1$ it follows from the fact that $f(x)=x/\ln(x+1)$ is an increasing function of x. □

Note 2.6.13. The limit in (2.6.7) follows directly from Legendre's formula

$$\nu_p(n!) = \frac{n-s_p(n)}{p-1} \tag{2.6.9}$$

and Exercise 2.6.5.

2.7. The central binomial coefficients

For fixed $m \in \mathbb{N}$, the row of binomial coefficients $\{\binom{m}{k} : 0 \leq k \leq m\}$ has $m+1$ terms. For m even, there is a central term that has interesting arithmetical and combinatorial properties. This section presents some of them.

Definition 2.7.1. The **central binomial coefficient** is given by

$$c_n := \binom{2n}{n}. \tag{2.7.1}$$

Warning: This number should not be confused with the **Catalan number** C_n defined in Chaper 6.

Exercise 2.7.2. The central binomial coefficient c_n satisfies

$$(n+1)c_{n+1} = 2(2n+1)c_n. \tag{2.7.2}$$

Prove that

$$\lim_{n\to\infty}\frac{c_{n+1}}{c_n} = 4 \tag{2.7.3}$$

with and without using (2.7.2).

2.7.1. The generating function of the central binomial coefficients. An explicit formula for the generating function

$$C(x) = \sum_{n=0}^{\infty} c_n x^n \tag{2.7.4}$$

is presented here. The proof follows the paper by J. Brown and V. E. Hoggart [**81**].

Theorem 2.7.3. *The generating function of the central binomial coeffcients is given by*

$$C(x) = \sum_{n=0}^{\infty} c_n x^n = \frac{1}{\sqrt{1-4x}}. \tag{2.7.5}$$

Proof. Differentiate to produce

$$C'(x) = \sum_{n=0} n c_n x^{n-1} = \sum_{n=0}^{\infty} (n+1) c_{n+1} x^n \tag{2.7.6}$$

and (2.7.2) gives

$$\begin{aligned} C'(x) &= \sum_{n=0}^{\infty} 2(2n+1) c_n x^n \\ &= 2\left(\sum_{n=0}^{\infty} 2n c_n x^n + \sum_{n=0}^{\infty} c_n x^n \right). \end{aligned}$$

This gives

$$\frac{C'(x)}{C(x)} = \frac{2}{1-4x}. \tag{2.7.7}$$

Integrating and using $C(0) = c_0 = 1$ yields the result. □

Exercise 2.7.4. Check the identity

$$\binom{2n}{n} = (-4)^n \binom{-\frac{1}{2}}{n}$$

and use the binomial theorem, Theorem 2.4.2, to provide a different proof of Theorem 2.7.3.

Note 2.7.5. The function $y = f(x)$ is called **algebraic** if there is a polynomial in two variables such that $P(x, f(x)) = 0$. The generating function of the central binomial coefficients (2.7.5) is algebraic.

Indeed, $y = 1/\sqrt{1-4x}$ satisfies $(1-4x)y^2 - 1 = 0$. The generating function for the Catalan numbers (6.3.2) and the one for central trinomial coefficients (2.11.12) are also algebraic. Examples of sequences whose generating functions are not algebraic include the harmonic numbers (11.11.3), the derangement numbers (11.7.8), and the numbers $B_n/n!$ with B_n the Bernoulli numbers (13.2.1). Theorem 8.3.1 presents a characterization of sequences with rational generating functions. There seems to be no simple analog for the algebraic case. Examples of sequences with algebraic generating functions are the topic of current research: see for instance the papers by A. Bostan and M. Kauers [**73**] and M. Bousquet-Melou [**74**].

2.7.2. Divisibility properties of c_n.

Some arithmetical properties of the central binomial coefficients are considered next.

Theorem 2.7.6. *The central binomial coefficient c_n is always even. Moreover $\frac{1}{2}c_n$ is odd if and only if n is a power of 2.*

Proof. The number c_n satisfies

$$c_n = \binom{2n}{n} = \binom{2n-1}{n} + \binom{2n-1}{n-1}$$

and the symmetry of the binomial coefficients yields

$$c_n = 2\binom{2n-1}{n}, \tag{2.7.8}$$

showing that c_n is even.

Legendre's series (2.6.1) yields

$$\nu_2((2n)!) = \sum_{k=1}^{\infty} \left\lfloor \frac{2n}{2^k} \right\rfloor = n + \nu_2(n!);$$

therefore

$$\nu_2(c_n) = n - \nu_2(n!).$$

Thus $\frac{1}{2}\binom{2n}{n}$ is odd if and only if

$$\sum_{k=1}^{\infty} \left\lfloor \frac{n}{2^k} \right\rfloor = n - 1. \tag{2.7.9}$$

The claim is that (2.7.9) implies n must be a power of 2. Three proofs are presented, with two of them as exercises.

Proof. First obseve that the term n in (2.7.9) can be replaced by its odd part. Indeed, writing $n = 2^a \cdot b$ with a and b positive integers and b odd, (2.7.9) is equivalent to

$$\begin{aligned} 2^a \cdot b - 1 &= \sum_{k=1}^{\infty} \left\lfloor \frac{b}{2^{k-a}} \right\rfloor \\ &= \sum_{k=1-a}^{\infty} \left\lfloor \frac{b}{2^k} \right\rfloor \\ &= \sum_{k=1-a}^{0} \left\lfloor \frac{b}{2^k} \right\rfloor + \sum_{k=1}^{\infty} \left\lfloor \frac{b}{2^k} \right\rfloor \\ &= b(2^a - 1) + \sum_{k=1}^{\infty} \left\lfloor \frac{b}{2^k} \right\rfloor . \end{aligned}$$

Thus,

$$\sum_{k=1}^{\infty} \left\lfloor \frac{b}{2^k} \right\rfloor = b - 1. \tag{2.7.10}$$

This is (2.7.9) with n replaced by its odd part b.

It remains to show that (2.7.10) implies $b = 1$. Clearly (2.7.10) holds for $b = 1$. If $b > 1$, then there exists a positive integer N such that $2^N < b < 2^{N+1}$, and (2.7.10) becomes

$$\sum_{k=1}^{N} \left\lfloor \frac{b}{2^k} \right\rfloor = b - 1, \tag{2.7.11}$$

but for $b \geq 3$ (and odd),

$$b - 1 = \sum_{k=1}^{N} \left\lfloor \frac{b}{2^k} \right\rfloor = \sum_{k=1}^{N} \left\lfloor \frac{b-1}{2^k} \right\rfloor \leq (b-1)(1 - 2^{-N}) \leq b - 2.$$

This is a contradiction. It follows that $b = 1$ and thus n is a power of 2. □

The next two exercises outline two alternative proofs.

Exercise 2.7.7. Check the details of the following argument: observe that $n \geq \nu_2(n!)$, $\nu_2((2^m)!) = 2^{m-1} + 2^{m-2} + \cdots + 1 = 2^m - 1$, and if a is the largest integer such that $n = 2^a + b$, then

$$\nu_2(n!) = \nu_2((2^a)!) + \nu_2(b!) = 2^a - 1 + \nu_2(b!).$$

Now for $n = 2^a$,

$$\nu_2(c_n) = 2^a - \nu_2(2^a!) = 2^a - (2^a - 1) = 1,$$

and for $n = 2^a + b$ $(0 < b < 2^a)$,

$$\begin{aligned} \nu_2(c_n) &= 2^a + b - \nu_2((2^a + b)!) \\ &= 2^a + b - (2^a - 1 + \nu_2(b!)) \\ &> b + 1 - b = 1. \end{aligned}$$

This gives the result.

Exercise 2.7.8. The result follows from $\nu_2(c_n) = s_2(n)$. This follows easily from Legendre's formula (2.6.3).

2.7.3. Primes dividing the central binomial coefficients.

Theorem 2.6.7 gives the expression

$$\nu_p\left(c_n\right) = \sum_{j \geq 0} \varepsilon_j$$

where ε_j is the carry in the jth digit when adding n to itself. This formula directly gives the next result.

Theorem 2.7.9. *A prime p divides the central binomial coefficient c_n if and only if there is a digit of n in its base p expansion that is at least $p/2$.*

Corollary 2.7.10. *Every prime divides some central binomial coefficient.*

Note 2.7.11. The central binomial coefficients are generalized by

$$c(n,k) = \frac{k^n}{n!} \prod_{m=1}^{n-1} (1 + km). \tag{2.7.12}$$

The numbers $c(n,k)$ are integers and $c(n,2) = c_n$. The generating function for $c(n,k)$ is

$$\sum_{n=0}^{\infty} c(n,k) x^n = (1 - k^2 x)^{-1/k}.$$

For p prime, the p-adic valuation of $c(n,k)$ is given by

$$\nu_p(c(n,k)) = n\nu_p(k) - \frac{n - s_p(n)}{p-1}$$

if p divides k, with $s_p(n)$ the sum of p-digits of n. An expression for the case when p does not divide k as well as proofs of the statements given here appear in a paper by T. Amdeberhan, V. Moll, and A. Straub [**283**].

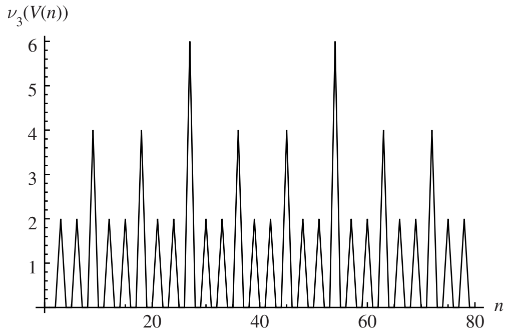


Figure 2.7.1. The 3-adic valuation of $V_n = u_n/\binom{2n}{n}$.

Note 2.7.12. The 3-adic valuations of the sums

$$u_n := \sum_{k=0}^{n-1} \binom{2k}{k}$$

were discussed by D. Zagier in [**284**] in response to a problem proposed by N. Strauss and J. Shallit. The result established there is that

$$\nu_3(u_n) = 2\nu_3(n) + \nu_3\binom{2n}{n}.$$

The existence of such a nice formula is linked to the regularity of the graph seen in Figure 2.7.1. This figure shows $\nu_3(V_n)$, where $V_n = u_n/\binom{2n}{n}$. Compare Figure 2.7.2, which shows the corresponding values for $p = 5$ and $p = 7$.

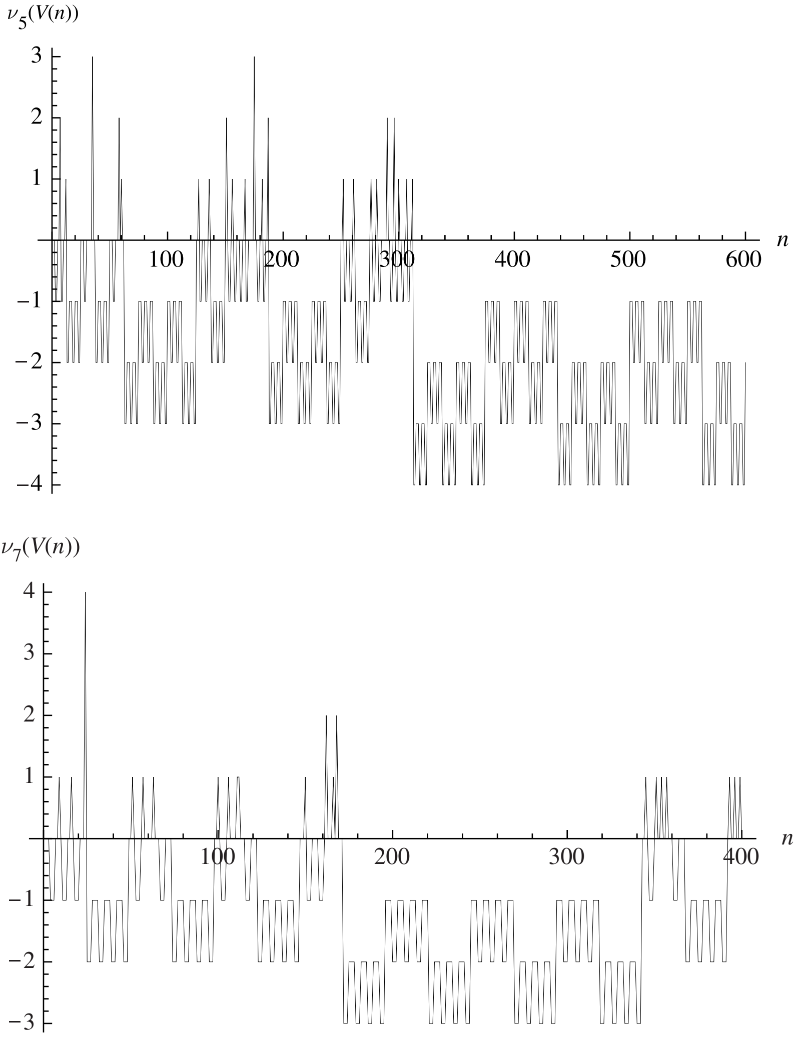


Figure 2.7.2. The 5- and 7-adic valuations of $V_n = u_n/\binom{2n}{n}$.

2.8. Bertrand's postulate

The arithmetic properties of central binomial coefficients were employed by P. Erdös to provide a proof of **Bertrand's postulate**.

This statement, given in Theorem 2.8.1, was conjectured in 1845 and proved by Tchebyshev in 1850.

Theorem 2.8.1. ***Bertrand's postulate.*** *For any $n \in \mathbb{N}$, there is a prime p such that $n < p \leq 2n$.*

Naturally the upper bound $2n$ is only achieved for $n = 1$. The proof presented follows the presentation given by D. Galvin [**132**].

Exercise 2.8.2. Prove the inequality

$$\binom{2n}{n} \geq \frac{4^n}{2n+1}. \tag{2.8.1}$$

Hint: Think of $(1+1)^{2n}$.

The next step is to analyze the p-adic valuation of $\binom{2n}{n}$. It is clear that any prime divisor p of $\binom{2n}{n}$ must satisfy $p \leq 2n$. The next lemma excludes some of this range.

Lemma 2.8.3. *If $\frac{2n}{3} < p \leq n$, then $\nu_p\left(\binom{2n}{n}\right) = 0$; that is, p does not divide $\binom{2n}{n}$.*

Proof. For such p,

$$\nu_p\left(\binom{2n}{n}\right) = \nu_p((2n)!) - 2\nu_p(p!). \tag{2.8.2}$$

The first term is 2, since only p and $2p$ divide $(2n)!$. Similarly, the second term is 1. This gives the result. □

Now assume that there is no prime p in the interval $(n, 2n)$. Therefore all prime divisors of $\binom{2n}{n}$ are in $\left(2, \frac{2n}{3}\right)$. The next statement bounds the power of p in $\binom{2n}{n}$.

Lemma 2.8.4. *If p divides $\binom{2n}{n}$, then $\nu_p\left(\binom{2n}{n}\right) \leq \log_p(2n)$.*

Proof. Define $r(p)$ by the inequalities $p^{r(p)} \leq 2n < p^{r(p)+1}$. Then

$$\begin{aligned}
\nu_p\left(\binom{2n}{n}\right) &= \nu_p((2n)!) - 2\nu_p(n!) \\
&= \sum_{i=1}^{r(p)} \left(\left\lfloor \frac{2n}{p^i} \right\rfloor - 2\left\lfloor \frac{n}{p^i} \right\rfloor \right) \\
&\leq r(p),
\end{aligned}$$

because, for a, $b \in \mathbb{N}$, the bounds $0 \leq \lfloor 2a/b \rfloor - 2\lfloor a/b \rfloor \leq 1$ hold. □

The next result will help to bound $\binom{2n}{n}$.

Lemma 2.8.5. *For $n \in \mathbb{N}$ and the product running over primes,*

$$\prod_{p \leq n} p \leq 4^n.$$

Proof. The argument is by induction on n. If n is even and $n \geq 4$, then by induction

$$\prod_{p \leq n} p = \prod_{p \leq n-1} p \leq 4^{n-1} < 4^n.$$

On the other hand, if n is odd, say $n = 2m + 1$,

$$\prod_{p \leq n} p = \prod_{p \leq m+1} p \times \prod_{p=m+2}^{2m+1} p \leq 4^{m+1} \binom{2m+1}{m},$$

using the induction hypothesis on the first product and the fact that every prime between $m + 2$ and $2m + 1$ divides $\binom{2m+1}{m}$ to bound the second product. To finish the argument, now use the bound

$$\binom{2m+1}{m} \leq 2^{2m}. \tag{2.8.3}$$

This is left as an exercise. □

Exercise 2.8.6. Prove the bound (2.8.3). **Hint:** Use the identity

$$\sum_{i=0}^{2m+1} \binom{2m+1}{i} = 2^{2m+1}.$$

Proof of Bertrand's postulate. Assume that there is no prime p in the interval $n < p \leq 2n$. The central binomial coefficient $\binom{2n}{n}$ has at most $\sqrt{2n}$ prime factors that are smaller than $\sqrt{2n}$. Lemma 2.8.4 shows that each of those prime factors contributes at most $2n$ to $\binom{2n}{n}$.

Also every prime $p > \sqrt{2n}$ satisfies $\nu_p\left(\binom{2n}{n}\right) \leq 1$. This gives

$$\begin{aligned} \binom{2n}{n} & \leq (2n)^{\sqrt{2n}} \prod_{\sqrt{2n} < p \leq 2n/3} p \\ & \leq (2n)^{\sqrt{2n}} \prod_{p=2}^{2n/3} p \\ & \leq (2n)^{\sqrt{2n}} 4^{2n/3}. \end{aligned}$$

Combining this with Exercise 2.8.2 gives

$$\frac{4^n}{2n+1} \leq (2n)^{\sqrt{2n}} 4^{2n/3}, \tag{2.8.4}$$

which may be written as

$$4^{n/3} \leq (2n+1)\,(2n)^{\sqrt{2n}}. \tag{2.8.5}$$

Exercise 2.8.7. Check that (2.8.5) fails for $n \geq 468$. Complete the proof by checking Bertrand's postulate for $n \leq 467$.

2.9. Some generating functions involving valuations

This section discusses some generating functions for sequences related to the 2-adic valuation $\nu_2(n)$. An interesting relation to the classical **$3x+1$ problem** is reported.

Example 2.9.1. The generating function of $\nu_2(n)$ is

$$\sum_{n=1}^{\infty} \nu_2(n) x^n = \sum_{k=1}^{\infty} \frac{x^{2^k}}{1 - x^{2^k}}. \tag{2.9.1}$$

Proof. The right-hand side is

$$\sum_{k=1}^{\infty} \frac{x^{2^k}}{1 - x^{2^k}} = \sum_{k=1}^{\infty} \sum_{j=1}^{\infty} x^{j \cdot 2^k}.$$

To analyze the number of coefficients that produce exponent $n \in \mathbb{N}$, write $n = s \cdot 2^{\nu_2(n)}$ with s is odd. Then the index j, which yields $j \cdot 2^k = n$, is written as $j = r \cdot 2^u$ with r odd and $1 \leq u \leq \nu_2(n)$. Then k is uniquely determined as $k = \nu_2(n) - u$ and the odd parts must match, that is, $r = s$. Therefore, there are $\nu_2(n)$ choices. This establishes the result. □

Example 2.9.2. The generating function of $\nu_2(n!)$ is

$$\sum_{m=0}^{\infty} \nu_2(n!)x^n = \frac{1}{1-x}\sum_{k=1}^{\infty} \frac{x^{2^k}}{1-x^{2^k}}. \tag{2.9.2}$$

Proof. Use $\nu_2(n) = \nu_2(n!) - \nu_2((n-1)!)$ and Example 2.9.1. □

Example 2.9.3. The generating function of the numbers

$$a_n := \nu_2(n(n+1)) \tag{2.9.3}$$

is given by

$$\sum_{n=1}^{\infty} a_n x^n = (1+x)\sum_{k\geq 1} \frac{x^{2^k-1}}{1-x^{2^k}}. \tag{2.9.4}$$

Proof. The proof follows directly from Example 2.9.1. □

Note 2.9.4. It has been observed that the numbers a_n in (2.9.3) also appear in the so-called **$3x+1$ problem**. The discussion starts with a description of this classical problem.

Definition 2.9.5. The map T is defined by

$$T(x) = \begin{cases} \frac{x}{2} & \text{if } x \text{ is even,} \\ \frac{3x+1}{2} & \text{if } x \text{ is odd.} \end{cases} \tag{2.9.5}$$

The *orbit* of $n \in \mathbb{N}$ under T is the set

$$\mathfrak{O}(n) := \{n, T(n), T^2(n), \ldots\}. \tag{2.9.6}$$

The main conjecture is that **every orbit ends in the cycle** $1 \to 2 \to 1$. The reader will find an introduction to this problem in a paper by J. C. Lagarias [**189**]. Additional information may be found in the work by M. Chamberland [**94**] and also in [**190**]. These papers contain extensive bibliographies.

Theorem 2.9.6. *Let $n \in \mathbb{N}$. Then $a_n := \nu_2(n(n+1))$ is the first time at which the orbit $\mathfrak{O}(n)$ changes parity. That is,*

$$n \equiv T(n) \equiv T^2(n) \equiv \cdots \equiv T^{a_n-1}(n) \not\equiv T^{a_n}(n) \bmod 2.$$

Proof. Suppose n is odd and write it as $n = 2^j r - 1$, with r odd. Then

$$j = \nu_2(n+1) \quad \text{and} \quad r = \frac{n+1}{2^j} \tag{2.9.7}$$

are uniquely defined. Observe that $T(n) = T(2^j r - 1) = 3 \cdot 2^{j-1} r - 1$ and $T^i(n) = T^i(2^j r - 1) = 3^i \cdot 2^{j-i} r - 1$ for $i < j$. Finally, $T^j(n) = T^j(2^j r - 1) = 3^j r - 1$. To complete the proof, observe that

$$j = \nu_2(n+1) = \nu_2(n(n+1)) = r.$$

In the case n is even, write $n = 2^j n_0$, with n_0 odd. Then $T^i(n) = 2^{j-i} n_0$, for $0 \leq i < j$ and $T^j(n) = n_0$. The proof is completed by observing that $t = \nu_2(n) = \nu_2(n(n+1)) = m_0$. □

The theorem is illustrated in the case $n = 63$. In this case, $T(63) = 95$, $T^2(63) = 143$, $T^3(63) = 215$, $T^4(63) = 323$, $T^5(63) = 485$, and $T^6(63) = 728$. Thus,

$$\mathfrak{O}(63) = \{63, 95, 143, 215, 323, 485, \mathbf{728}, \ldots\}. \tag{2.9.8}$$

It takes six iterations to produce an even entry. This is consistent with $a_{63} = \nu_2((63)_2) = 6$.

Example 2.9.7. The generating function of $s_2(n)$ is

$$\sum_{n=0}^{\infty} s_2(n) x^n = \frac{1}{1-x} \sum_{k=0}^{\infty} \frac{x^{2^k}}{1 + x^{2^k}}. \tag{2.9.9}$$

Proof. Legendre's identity (2.6.3) yields $s_2(n) - s_2(n-1) = 1 - \nu_2(n)$. It follows that

$$\sum_{n=1}^{\infty} s_2(n) x^n - \sum_{n=1}^{\infty} s_2(n-1) x^n = \sum_{n=1}^{\infty} x^n - \sum_{n=1}^{\infty} \nu_2(n) x^n.$$

Example 2.9.1 shows that the stated formula is equivalent to

$$\frac{x}{1-x} - \sum_{k=1}^{\infty} \frac{x^{2^k}}{1 - x^{2^k}} = \sum_{k=0}^{\infty} \frac{x^{2^k}}{1 + x^{2^k}},$$

which can be written as

$$\frac{2x}{1-x} - \sum_{k=0}^{\infty} \frac{x^{2^k}}{1 - x^{2^k}} = \sum_{k=0}^{\infty} \frac{x^{2^k}}{1 + x^{2^k}}.$$

Combining the two sums produces the identity

$$\sum_{m=0}^{\infty} \frac{x^{2^m}}{1-x^{2^{m+1}}} = \frac{x}{1-x}. \tag{2.9.10}$$

In turn, this is equivalent to the fact that every positive integer n is of the form $k \cdot 2^i$, with k odd. □

2.10. The asymptotics of factorials: Stirling's formula

Two of the most basic constants of analysis, e and π, and the factorial function $n!$ considered in this chapter are related by a remarkable formula of Stirling:

$$n! \sim \sqrt{2\pi n}\, n^n e^{-n} \quad \text{as } n \to \infty. \tag{2.10.1}$$

The reader will find in D. Dominici [**112**] a description of the variety of proofs of (2.10.1) occurring in the literature, some of which are also presented in the book **Irresistible Integrals** [**65**].

In this chapter only the existence of the appropriate limit is established. The most basic properties of the logarithm function are employed. The value $\sqrt{2\pi}$ in (2.10.1) for the limit is postponed until Chapter 12 (see Exercise 12.6.4).

Theorem 2.10.1. *The limit*

$$A := \lim_{n\to\infty} \frac{n!}{e^{-n}n^{n+1/2}}$$

exists.

Proof. Adding the inequalities

$$\int_{k-1}^{k} \ln x\, dx < \ln k < \int_{k}^{k+1} \ln x\, dx$$

from $k=1$ to $k=n$ and using the identity

$$\ln n! = \ln 1 + \ln 2 + \cdots + \ln n$$

give

$$\int_0^n \ln x\, dx < \ln n! < \int_1^{n+1} \ln x\, dx.$$

Evaluating the integrals produces

$$n \ln n - n < \ln n! < (n+1)\ln(n+1) - n.$$

Define

$$t_n = \ln n! - \left(n + \tfrac{1}{2}\right)\ln n + n.$$

Then

$$t_n - t_{n+1} = \left(n + \tfrac{1}{2}\right)\ln\left(\frac{n+1}{n}\right) - 1.$$

The series

$$\frac{1}{2}\ln\left(\frac{1+t}{1-t}\right) = t + \frac{1}{3}t^3 + \frac{1}{5}t^5 + \cdots$$

is elementary (this is included as Exercise 11.8.5). It produces

$$t_n - t_{n+1} = \frac{1}{3}\frac{1}{(2n+1)^2} + \frac{1}{5}\frac{1}{(2n+1)^4} + \cdots,$$

which gives

$$0 < t_n - t_{n+1} < \frac{1}{3}\left(\frac{1}{(2n+1)^2} + \frac{1}{(2n+1)^4} + \cdots\right) = \frac{1}{12}\left(\frac{1}{n} - \frac{1}{n+1}\right).$$

The last step involves adding a geometric progression. This proves t_n is decreasing and $t_n - \frac{1}{12n}$ is increasing. It follows that t_n converges to a limit. Taking the exponential of t_n gives the result. □

Exercise 2.10.2. Use Stirling's formula to verify that

$$\lim_{n\to\infty} \frac{\sqrt{n}\binom{2n}{n}}{2^{2n}} = \frac{1}{\sqrt{\pi}}.$$

Exercise 2.10.3. Establish the result

$$\lim_{n\to\infty} (n!)^{1/n} = +\infty. \tag{2.10.2}$$

This is weaker than Stirling's formula, but it is much easier to establish. **Hint:** If the sequence $\{a_n\}$ tends to a limit (including $+\infty$ or $-\infty$), then the average $\frac{1}{n}(a_1 + \cdots + a_n)$ tends to the same limit. Apply this to $a_n = \ln n$.

2.11. The trinomial coefficients

The **trinomial coefficient** $T_{i,j,k}$ is defined by the expansion

$$(x+y+z)^n = \sum_{i,j,k} T_{i,j,k} x^i y^j z^k. \tag{2.11.1}$$

The term corresponding to those indices summing up to n is said to have **rank** n. It is denoted by TC_n.

Lemma 2.11.1. *The trinomial coefficient of rank n is given by*

$$TC_n = \sum_{i+j+k=n} \frac{n!}{i!\,j!\,k!}. \tag{2.11.2}$$

Proof. To count the coefficient of $x^i y^j z^k$ with $i+j+k=n$, multiply the n factors in (2.11.1). First choose the i terms from which the power of x comes. This can be done in $\binom{n}{i}$ ways. From the remaining $n-i$ factors, choose the positions of the j factors giving the power of y. This can be achieved in $\binom{n-i}{j}$. The remaining $n-i-j=k$ terms give the power of z. The total numbers of choices is

$$\binom{n}{i} \times \binom{n-i}{j} = \frac{n!}{i!\,j!\,k!} \tag{2.11.3}$$

as claimed. □

Exercise 2.11.2. Extend the previous argument to produce an expression for the coefficient of $x_1^{a_1} x_2^{a_2} \cdots x_r^{a_r}$ in the expansion of the multinomial $(x_1+x_2+\cdots+x_r)^n$ with fixed sum $a_1+a_2+\cdots+a_r=s$. The special case discussed above corresponds to $r=3$ and $s=n$.

The special case of the expansion

$$(1+x+x^2)^n = \sum_{i=0}^{2n} b_{i,n} x^i \tag{2.11.4}$$

is considered here. The coefficients $b_{i,n}$ are also called the **trinomial coefficients**. The reader should be careful with this notation since it is not standard.

Theorem 2.11.3. *The trinomial coefficients $b_{i,n}$ are given by*

$$b_{i,n} = \sum_{k=0}^{n} \binom{n}{k} \binom{n-k}{i-2k}. \tag{2.11.5}$$

Proof. It is clear that $(1+x+x^2)^n$ is a polynomial of degree $2n$. The binomial theorem gives

$$\begin{aligned}((1+x)+x^2)^n &= \sum_{k=0}^{n}\binom{n}{k}(1+x)^{n-k}x^{2k} \\ &= \sum_{k=0}^{n}\binom{n}{k}x^{2k}\sum_{j=0}^{n-k}\binom{n-k}{j}x^j \\ &= \sum_{k=0}^{n}\sum_{j=0}^{n-k}\binom{n}{k}\binom{n-k}{j}x^{2k+j}.\end{aligned}$$

The exponent of x satisfies the bounds $2k+j \leq 2k+n-k = n+k \leq 2n$. To simplify this sum, observe that the upper bound of j can be extended to n, since the terms with $n-k+1 \leq j \leq n$ vanish. Then

$$(1+x+x^2)^n = \sum_{k=0}^{n}\sum_{j=0}^{n}\binom{n}{k}\binom{n-k}{j}x^{2k+j}.$$

Let $i = 2k+j$ so that $0 \leq i \leq 2n$. Then

$$(1+x+x^2)^n = \sum_{i=0}^{2n}\left(\sum_{k=0}^{n}\binom{n}{k}\binom{n-k}{i-2k}\right)x^i.$$

The expression for $b_{i,n}$ follows from here. □

Corollary 2.11.4. *The trinomial coefficients $b_{i,n}$ are symmetric; that is,*

$$b_{2n-i,n} = b_{i,n}, \quad \text{for } 0 \leq i \leq 2n. \tag{2.11.6}$$

Proof. The chain of identities

$$\begin{aligned}\sum_{i=0}^{2n} b_{2n-i}x^i &= \sum_{j=0}^{2n} b_j x^{2n-j} \\ &= x^{2n}\sum_{j=0}^{2n} b_j x^{-j} \\ &= x^{2n}(1+x^{-1}+x^{-2})^{2n} \\ &= (1+x+x^2)^n\end{aligned}$$

gives the result. □

Definition 2.11.5. The **central trinomial coefficients** are defined by $b_n := b_{n,n}$. This is entry $A002426$ in OEIS.

The expression for $b_{i,n}$ as a double sum gives the next statement.

Corollary 2.11.6. *The central trinomial coefficient b_n is given by*

$$b_n = \sum_{k=0}^{\lfloor n/2 \rfloor} \binom{n}{k} \binom{n-k}{n-2k} = \sum_{k=0}^{\lfloor n/2 \rfloor} \binom{n}{k} \binom{n-k}{k}. \tag{2.11.7}$$

These are also given by

$$b_n = \sum_{k=0}^{\lfloor n/2 \rfloor} \binom{n}{2k} \binom{2k}{k}. \tag{2.11.8}$$

Proof. The last identity follows from

$$\binom{n}{k} \binom{n-k}{k} = \binom{n}{2k} \binom{2k}{k}. \tag{2.11.9}$$

□

Exercise 2.11.7. Prove that b_n is the number of permutations of n symbols taken from $\{-1, 0, 1\}$ with vanishing total sum.

Note 2.11.8. The first few values of the central trinomial coefficients are

$$1,\ 1,\ 3,\ 7,\ 19,\ 51,\ 141,\ 393,\ 1107.$$

A search in Sloane's database finds these numbers in relation to the recurrence

$$a_{n+1} = 3a_n - F_n(F_n + 1), \quad a_0 = 1, \tag{2.11.10}$$

where the F_n are the Fibonacci numbers studied in Chapter 3. The first nine values of a_n and b_{n+1} agree. **Is there an explanation for this coincidence?**

Note 2.11.9. The methods developed by H. Wilf and D. Zeilberger show that b_n is not the sum of a fixed number of hypergeometric terms. See [**247**, page 160].

2.11.1. The Hausdorff moment problem. Given a sequence of numbers μ_n, the *Hausdorff moment problem* asks for necessary and sufficient conditions on the sequence in order that there exists a distribution function Φ on a fixed interval $[a, b]$ such that

$$\mu_n = \int_a^b x^n d\Phi(x).$$

The reader may simply think of $d\Phi(x)$ as given by the form $\varphi(x)dx$.

The next exercise presents the solution of the Hausdorff moment problem for the central trinomial coefficients.

Exercise 2.11.10. Prove that

$$b_n = \frac{1}{\pi} \int_{-1}^{3} \frac{x^n \, dx}{\sqrt{(3-x)(x+1)}} = \frac{1}{\pi} \int_{-1}^{1} \frac{(2u+1)^n \, du}{\sqrt{1-u^2}}.$$

Expand the integrand and use Wallis' formula

$$\int_0^\infty \frac{dx}{(x^2+1)^{m+1}} = \int_0^{\pi/2} \cos^{2m}\theta \, d\theta = \frac{\pi}{2^{2m+1}} \binom{2m}{m} \tag{2.11.11}$$

to recover (2.11.8). Chapter 9 is dedicated to formula (2.11.11).

2.11.2. Generating function for central trinomial coefficients. The generating function for the sequence $\{b_n\}$ is established now. The proof employs the next exercise. The explicit formula derived here shows that, as in the case of the central binomial coefficients, the central trinomial coefficients have an algebraic generating function.

Exercise 2.11.11. Establish the expansion

$$\frac{x^j}{(1-x)^{j+1}} = \sum_{m=0}^{\infty} \binom{m}{j} x^m. \tag{2.11.12}$$

Hint: Define $f(x) = x^j/(1-x)^{j+1}$. Prove that the function $Q_n(x)$ defined by

$$Q_n(x) = (1-x)^{n+1+j} x^{n-j} \left(\frac{d}{dx} \right)^n f(x)$$

satisfies the recurrence

$$Q_{n+1}(x) = -x(x-1)Q_n'(x) + \left[(2n+1)x - (n-j) \right] Q_n(x).$$

Conclude that $Q_n(x)$ is a polynomial in x. Now use it to evaluate the derivatives of f at $x = 0$.

Theorem 2.11.12. *The generating function of the central trinomial coefficients $\{b_n\}$ is given by*

$$CT(x) = \frac{1}{\sqrt{1-2x-3x^2}}.$$

Proof. Start with

$$\begin{aligned} CT(x) &= \sum_{m=0}^{\infty} b_m x^m \\ &= \sum_{k=0}^{\infty} \left(\sum_{m=2k}^{\infty} \binom{m}{2k} x^m \right) \binom{2k}{k} \\ &= \sum_{k=0}^{\infty} \binom{2k}{k} \sum_{m=0}^{\infty} \binom{m}{2k} x^m. \end{aligned}$$

Exercise 2.11.11 gives

$$CT(x) = \sum_{m=0}^{\infty} \binom{2k}{k} \frac{x^{2k}}{(1-x)^{2k+1}}. \tag{2.11.13}$$

Now recall the generating function of the central binomial coefficients

$$A(x) = \sum_{k=0}^{\infty} \binom{2k}{k} x^k = \frac{1}{\sqrt{1-4x}},$$

and observe the relation

$$CT(x) = \frac{1}{1-x} A\left(\frac{x^2}{(1-x)^2} \right), \tag{2.11.14}$$

which simplifies to give the stated formula. □

2.11.3. A recurrence for the central trinomial coefficients.

A recurrence for the central trinomial coefficients is established next. Two elementary proofs are given as Exercises 2.11.14 and 2.11.15. The more complicated proof presented here employs the polynomials $b_n(t)$ defined by the generating function

$$\sum_{n=0}^{\infty} b_n(t) x^n = \frac{1}{\sqrt{1-2xt-3x^2}}. \tag{2.11.15}$$

The recurrence comes from the specialization $b_n = b_n(1)$. These polynomials can be expressed in terms of the Legendre polynomials described in Chapter 14.

Theorem 2.11.13. *The central trinomial coefficients b_n satisfy*

$$nb_n = (2n-1)b_{n-1} + 3(n-1)b_{n-2}. \tag{2.11.16}$$

Proof. The idea is to employ the generating function for the Legendre polynomials

$$\sum_{n=0}^{\infty} P_n(t)x^n = \frac{1}{\sqrt{1-2xt+x^2}}. \tag{2.11.17}$$

The generating function appears in Theorem 14.2.32.

Consider the two-parameter function

$$CT(x,t) = \frac{1}{\sqrt{1-2xt-3x^2}} = \sum_{n=0}^{\infty} b_n(t)x^n. \tag{2.11.18}$$

Then $CT(x,1) = CT(x)$ and $b_n(1) = b_n$. In order to convert the problem to the Legendre polynomial format, write

$$1-2xt-3x^2 = 1-2x_1t_1+x_1^2$$

with $x_1 = -i\sqrt{3}x$ and $t_1 = it/\sqrt{3}$. Then

$$\sum_{n=0}^{\infty} b_n(t)x^n = \sum_{n=0}^{\infty} P_n(t_1)x_1^n,$$

and therefore

$$b_n = (-i\sqrt{3})^n P_n\left(\frac{i}{\sqrt{3}}\right).$$

The recursion for Legendre polynomials, given in Theorem 14.2.16, is

$$nP_n(x) = (2n-1)xP_{n-1}(x) - (n-1)P_{n-2}(x) \tag{2.11.19}$$

with $P_0(x) = 1$ and $P_1(x) = x$. The recurrence for b_n follows from (2.11.19). □

Exercise 2.11.14. Give a direct proof of this recurrence by showing that the generating function of the central trinomial coefficients $f(x)$ satisfies the differential equation

$$(3x+1)f(x) + (3x^2+2x-1)f'(x) = 0.$$

Exercise 2.11.15. Give an even easier proof of the recurrence for central trinomial coefficients by using the WZ-machinery (for Wilf-Zeilberger).

The next corollary is the analog of (2.7.3).

Corollary 2.11.16. *Assume that the limit*

$$L = \lim_{n\to\infty} \frac{b_{n+1}}{b_n}$$

exists. Then $L = 3$.

Proof. The limit gives the reciprocal of the radius of convergence of the generating function of $\{b_n\}$. The explicit formula given in Theorem 2.11.12 gives the result. □

Exercise 2.11.17. Obtain the value of the limit directly from the recurrence (2.11.16). **Warning:** In order to be fair to the reader, the author wishes to state that he has not checked the details of this exercise.

2.11.4. From the recurrence to the generating function. The goal is now to produce the generating function (2.11.12) directly from the recurrence (2.11.16). This is written in shifted form as

$$(n+2)b_{n+2} = (2n+3)b_{n+1} + 3(n+1)b_n. \tag{2.11.20}$$

Multiply (2.11.20) by x^n and sum to produce

$$\sum_{n=0}^{\infty}(n+2)b_{n+2}x^n = \sum_{n=0}^{\infty}(2n+3)b_{n+1}x^n + \sum_{n=0}^{\infty} 3(n+1)b_nx^n.$$

To simplify these expressions, observe that

$$\sum_{n=0}^{\infty}(n+2)b_{n+2}x^n = \sum_{n=2}^{\infty} nb_nx^{n-2} = \frac{1}{x}\left(CT'(x) - b_1\right)$$

and

$$\sum_{n=0}^{\infty}(2n+3)b_{n+1}x^n = \sum_{n=1}^{\infty}(2n+1)b_nx^{n-1} = 2CT'(x) + \frac{1}{x}\left(CT(x) - b_0\right)$$

and finally

$$\sum_{n=0}^{\infty} 3(n+1)b_nx^n = 3xCT'(x) + 3CT(x).$$

This produces

$$CT'(x) - b_1 = 2xCT'(x) + CT(x) - b_0 + 3x^2CT'(x) + 3xCT(x)$$

and using $b_0 = b_1 = 1$ yields

$$\frac{CT'(x)}{CT(x)} = \frac{3x+1}{1-2x-3x^2}.$$

Integration and the value $CT(0) = 1$ give

$$CT(x) = \frac{1}{\sqrt{1-2x-3x^2}}.$$

2.11.5. Primes dividing the central trinomial coefficients.

The statement that every prime divides some central binomial coefficient given as Corollary 2.7.10 leads naturally to consider the list of primes that divide some b_n. Some of them are in the list

$$\{3, 7, 17, 19, 41, 43, 47, 73, 107, 109, 113, 131, 173, 179, 191, 193, \ldots\}.$$

This sequence appears as $A113304$ in OEIS. The author has been unable to find any property characterizing these primes.

At least the case of the prime $p = 2$ is relatively simple.

Exercise 2.11.18. Prove that the central trinomial coefficient is always odd.

Chapter 3

The Fibonacci Numbers

3.1. Introduction

The sequence of **Fibonacci numbers** defined by the recurrence

$$F_n = F_{n-1} + F_{n-2}, \qquad \text{for } n \in \mathbb{N},\ n \geq 3, \tag{3.1.1}$$

with the initial conditions $F_1 = 1$ and $F_2 = 1$, has appeared in Exercise 1.5.12 in the context of optimal length for the computation of greatest common divisor and in Note 2.11.8 in a recurrence matching the initial terms of the central binomial coefficients.

This sequence has been very well studied. It even has its own journal: ***The Fibonacci Quarterly***. The many books containing historical information about the Fibonacci numbers F_n include V. E. Hoggatt Jr. [**174**], T. Koshy [**186**], M. Livio [**202**], A. S. Posamentier and I. Lehman [**249**], and N. N. Vorob′ev [**301**]. This chapter contains some elementary properties of these numbers.

Note 3.1.1. The recurrence (3.1.1) may be employed to define F_n for $n \leq 0$ in a consistent manner. For example, the value $n = 2$ in the recurrence forces the definition $F_0 = 0$. This could be continued to produce $F_{-1} = 1$, $F_{-2} = -1$, $F_{-3} = 2$ and F_{-n} may be computed for all $n \in \mathbb{N}$.

3.2. What do they count?

The wonderful book by A. Benjamin and J. Quinn [**46**] begins the discussion on counting techniques with the following question:

How many sequences of 1***'s and*** 2***'s sum to*** n***?*** Denote the answer by f_n and observe that $f_4 = 5$ since

$$1+1+1+1 = 1+1+2 = 1+2+1 = 2+1+1 = 2+2 \tag{3.2.1}$$

are all such sequences. To obtain a recurrence for f_n, consider the first term x_1: the sequences split into two disjoint cases according to whether $x_1 = 1$ or $x_1 = 2$. In the former case, x_1 is complemented by the f_{n-1} sequences adding to $n-1$, in the latter by the f_{n-2} sequences adding to $n-2$. The addition principle gives

$$f_n = f_{n-1} + f_{n-2}. \tag{3.2.2}$$

It follows that f_n satisfies the same recurrence as the Fibonacci numbers. The coincidence of the initial values $f_1 = F_2$, $f_2 = F_3$ and Exercise 3.2.1 show that $f_n = F_{n+1}$.

Exercise 3.2.1. Prove that the second-order recurrence

$$x_n = ax_{n-1} + bx_{n-2}, \tag{3.2.3}$$

with constant coefficients a, b, is completely determined by the initial values x_1 and x_2. Find a formula for x_n in terms of the data $\{a, b, x_1, x_2\}$. **Hint:** Try a solution of the form $x_n = t^n$, for some t to be determined. Two values $t_{\pm}$ will appear. Then show that any solution must be a linear combination of t_+^n and t_-^n.

Note 3.2.2. Replacing the number 1 by a **square tile** and the number 2 by a **domino** of length 2, the previous result shows that the Fibonacci number F_{n+1} is the number of ways to tile a board of length n by tiles and dominos. The book [**46**] takes the tiling approach to the subject.

A second combinatorial problem leading to Fibonacci numbers is presented next.

Example 3.2.3. The number of subsets of $[n] := \{1, 2, \ldots, n\}$ that do not contain a pair of consecutive integers is given by F_{n+2}. To verify this statement, let G_n be the number of subsets satisfying the stated condition. For instance $G_2 = 3$ since the only subset of $\{1, 2\}$ violating the condition is $\{1, 2\}$. The sets A counted by G_n come in two types: those that contain n and those that do not. If $n \notin A$, then A is a subset of $[n-1]$. There are G_{n-1} of this type. On the other hand, if $n \in A$, then $n-1$ cannot be in A. Therefore $A \setminus \{n\} \subset [n-2]$ and there are G_{n-2} of this other type. The two types are exclusive and count all the sets. Therefore $G_n = G_{n-1} + G_{n-2}$. The matching of the initial conditions $G_1 = 2 = F_3$, $G_2 = 3 = F_4$ and Exercise 3.2.1 prove that $G_n = F_{n+2}$.

Example 3.2.4. Many properties of the Fibonacci numbers may be established by a combinatorial interpretation. An example illustrating the main idea is described now. The number f_{m+n} counts the ways to write $m+n$ as a sequence of 1's and 2's that add up to $m+n$. Compute the partial sums reading the sequence from left to right. There are sequences for which m appears as a partial sum and others for which $m-1$ is a partial sum, followed by a 2. For example, if $n = 5$ and $m = 7$, the sum $1+2+2+1+1+2+2+1$ is of the first type and $2+1+1+2+2+1+1+2$ is of the second type. There are $f_n f_m$ of the first type and $f_{m-1} f_{n-1}$ of the second type. Shifting the indices and using $f_n = F_{n+1}$ yields the identity

$$F_{n+m} = F_n F_{m+1} + F_{n-1} F_m. \tag{3.2.4}$$

Exercise 3.2.5. The Cassini identity

$$F_{n+1}^2 - F_{n+2} F_n = (-1)^n \tag{3.2.5}$$

can be established by induction. M. Werman and D. Zeilberger [**310**] gave a nice combinatorial proof. Define

$$A_n = \{(a_1, \ldots, a_r) : r \geq 0,\ a_i = 1 \text{ or } 2, \text{ and } a_1 + a_2 + \cdots + a_r = n\}.$$

Then $|A_n| = F_{n+1}$. Define a map $\psi : A_n \times A_n \to A_{n-1} \times A_{n+1}$ excluding the vector with $a_i = 2$, for all i. Write the pair $u = (a_1, a_2, \ldots, a_r), (b_1, \ldots, b_s)$ as the string $a_1, b_1, a_2, b_2, \ldots$. If the first 1 is a_k, delete a_k from the first vector and insert it between b_{k-1} and b_k. If the first 1 is b_k, then $a_k = 2$. Exchange a_k and b_k. Check that the map ψ is well-defined and that it gives a proof of Cassini's identity.

3.3. The generating function

The sequence of Fibonacci numbers $\{F_n\}$ has a very simple generating function. The explicit form of this function makes it a very important tool in the study of this sequence. In this section, the generating function

$$F(x) := \sum_{n=0}^{\infty} F_n x^n \tag{3.3.1}$$

is computed and some applications are presented.

Theorem 3.3.1. *The generating function of the Fibonacci numbers is given by*

$$F(x) = \frac{x}{1-x-x^2}. \tag{3.3.2}$$

Proof. Multiply (3.1.1) by x^n to produce

$$F_n x^n = x \times F_{n-1}x^{n-1} + x^2 \times F_{n-2}x^{n-2}, \quad \text{for } n \geq 2. \tag{3.3.3}$$

Recall that the value $F_0 = 0$ has been defined. Now sum from $n = 2$ on to produce

$$\sum_{n=2}^{\infty} F_n x^n = x \sum_{n=2}^{\infty} F_{n-1}x^{n-1} + x^2 \sum_{n=2}^{\infty} F_{n-2}x^{n-2}. \tag{3.3.4}$$

Shifting the index of summation yields

$$\sum_{n=2}^{\infty} F_n x^n = x \sum_{n=1}^{\infty} F_n x^n + x^2 \sum_{n=0}^{\infty} F_n x^n. \tag{3.3.5}$$

This can be expressed as

$$F(x) - F_0 - F_1 x = x\left(F(x) - F_0\right) + x^2 F(x), \tag{3.3.6}$$

and using $F_0 = 0$ and $F_1 = 1$ gives the result. □

Note 3.3.2. Section 8.3 shows that the fact that the generating function for Fibonacci numbers is a rational function is part of a general phenomenon. It is established that a sequence $\{a_n\}$ has a rational generating function if and only if it satisfies a linear recurrence with constant coefficients. The sequence of Fibonacci numbers and its generating function $F(x)$ illustrate this result.

The generating function (3.3.2) is employed now to obtain an explicit expression for the Fibonacci numbers. The zeros of the denominator of $F(x) = x/(1-x-x^2)$ are

$$\varphi_+ = \frac{\sqrt{5}-1}{2} \quad \text{and} \quad \varphi_- = -\frac{\sqrt{5}+1}{2}. \tag{3.3.7}$$

The relation $\varphi_+ \cdot \varphi_- = -1$ is useful in simplifications. Observe that φ_- is the negative of the golden ratio $\varphi = (\sqrt{5}+1)/2$ appearing in Exercise 1.9.23.

To use the method of partial fractions, it is convenient to write

$$\begin{aligned}\frac{x}{1-x-x^2} &= \frac{-x}{(1-x/\varphi_-)(1-x/\varphi_+)\varphi_-\varphi_+} \\ &= \frac{x}{(1-x/\varphi_-)(1-x/\varphi_+)}.\end{aligned}$$

The decomposition

$$\frac{x}{(1-x/\varphi_-)(1-x/\varphi_+)} = \frac{A}{1-x/\varphi_-} + \frac{B}{1-x/\varphi_+}$$

leads to the system of equations

$$A+B=0 \quad \text{and} \quad A/\varphi_+ + B/\varphi_- = -1.$$

The last equation is equivalent to $A\varphi_- + B\varphi_+ = 1$. The solution is

$$A = -1/\sqrt{5} \quad \text{and} \quad B = 1/\sqrt{5}. \tag{3.3.8}$$

It follows that

$$\frac{x}{1-x-x^2} = -\frac{1}{\sqrt{5}}\frac{1}{1+x\varphi_+} + \frac{1}{\sqrt{5}}\frac{1}{1+x\varphi_-}.$$

Expanding the terms $1/(1+x\varphi_\pm)$ as a geometric series gives the statement of the next theorem.

Theorem 3.3.3. *The Fibonacci numbers F_n are given by*

$$F_n = \frac{1}{\sqrt{5}}\left(\frac{\sqrt{5}+1}{2}\right)^n - \frac{(-1)^n}{\sqrt{5}}\left(\frac{\sqrt{5}-1}{2}\right)^n, \tag{3.3.9}$$

*for $n \geq 0$. This is called **Binet's formula**.*

Note 3.3.4. In terms of the roots $\varphi_\pm$, the previous result is written as

$$F_n = \frac{(-1)^n}{\sqrt{5}}\left[\varphi_-^n - \varphi_+^n\right]. \tag{3.3.10}$$

Corollary 3.3.5. *As $n \to \infty$, the Fibonacci numbers satisfy*

$$F_n \sim \frac{1}{\sqrt{5}}\varphi^n \qquad \text{with } \varphi = \frac{\sqrt{5}+1}{2}.$$

Exercise 3.3.6. Prove that F_n is the integer closest to $\frac{1}{\sqrt{5}}\varphi^n$.

Exercise 3.3.7. Evaluate the continued fraction of the quotient of two consecutive Fibonacci numbers. Describe the relation

$$\lim_{n\to\infty} \frac{F_{n+1}}{F_n} = \varphi$$

from the point of view of continued fractions.

Exercise 3.3.8. Discuss how useful Binet's formula is for actually computing the nth Fibonacci number.

Exercise 3.3.9. Prove identity (3.2.4) by using the generating function of the Fibonacci numbers. **Hint:** Multiply by $x^n y^m$ and sum over all n, $m \in \mathbb{N}$.

Exercise 3.3.10. Binet's formula reduces the verification of many of the relations among Fibonacci numbers to an algebraic problem involving the roots $\varphi_\pm$. Use this procedure to check the following **Pythagorean relations**:

(1) If $a_n = F_{2n-1}$, $b_n = 2F_nF_{n-1}$, and $c_n = F_n^2 - F_{n-1}^2$, then $a_n^2 = b_n^2 + c_n^2$.

(2) If $a_n = F_nF_{n+3}$, $b_n = 2F_{n+1}F_{n+2}$, and $c_n = F_{2n+3}$, then $a_n^2 + b_n^2 = c_n^2$.

3.4. A family of related numbers

A companion sequence to $\{F_n\}$ is obtained by modifying the initial conditions in the recurrence (3.1.1) that defined the Fibonacci numbers.

Definition 3.4.1. The **Lucas numbers** L_n are defined by the recurrence

$$L_n = L_{n-1} + L_{n-2} \tag{3.4.1}$$

and the initial conditions $L_1 = 1$ and $L_2 = 3$.

Proceeding as in the proof of Theorem 3.3.3 yields the next result. Compare this with (3.3.10).

Theorem 3.4.2. *The Lucas numbers are given by*

$$L_n = (-1)^n \left(\varphi_+^n + \varphi_-^n \right). \tag{3.4.2}$$

Exercise 3.4.3. Prove that, for $n,\, m \in \mathbb{N}$,

$$2F_{n+m} = F_n L_m + F_m L_n. \tag{3.4.3}$$

This can be checked by the explicit formulas for Fibonacci and Lucas numbers. Give a combinatorial proof also. **Hint:** Tile a board of length $m+n$ with square tiles or domino tiles. The tilings are divided into two types according to whether there is a domino covering the cells m and $m+1$.

Exercise 3.4.4. Establish the relation $F_{2n} = F_n L_n$.

Exercise 3.4.5. Prove that L_n is the integer closest to φ^n.

Exercise 3.4.6. Define the numbers $V_n(a,b)$ by the recurrence

$$V_n(a,b) = V_{n-1}(a,b) + V_{n-2}(a,b) \tag{3.4.4}$$

with initial conditions $V_1(a,b) = a$ and $V_2(a,b) = b$. This family includes the Fibonacci numbers, for which $a = b = 1$, and the Lucas numbers, for which $a = 1$ and $b = 3$. Introduce

$$q_n(a,b) = \frac{V_{n+1}(a,b)}{V_n(a,b)}, \tag{3.4.5}$$

and let s be the continued fraction of $q_1(a,b)$. Prove that the continued fraction of $q_n(a,b)$ has the form $[1, 1, \ldots, 1, s]$ where there are $n-1$ 1's at the beginning.

Note 3.4.7. The Lucas numbers play an important role in the quest for the largest prime numbers known. The **Mersenne number** is $M_n = 2^n - 1$. If $n = a \cdot b$, with $a, b > 1$, then M_a divides M_n. Therefore, in order for M_n to be prime, n itself must be prime. For p prime, if the number M_p is prime, it is called a **Mersenne prime**. Unfortunately, not all M_p are prime. The first composite M_p's are

$$M_{11} = 23 \cdot 89, \quad M_{23} = 47 \cdot 178481, \quad \text{and} \quad M_{29} = 233 \cdot 1103 \cdot 2089.$$

E. Lucas proposed a criterion for primality of M_p. A rigorous proof was provided by D. H. Lehmer. A very readable proof of the next theorem appears in the paper by J. H. Jaroma [**179**]. The reader will also enjoy reading the papers by J. W. Bruce [**83**] and by M. I. Rosen [**258**]. These papers require only a minimal background in algebra.

Theorem 3.4.8. *Define the sequence* $\{s_i\}$ *by* $s_0 = 4$ *and* $s_i = s_{i-1}^2 - 2$ *and let* p *be prime. Then* M_p *is prime if and ony if* $s_{p-2} \equiv 0 \bmod M_p$.

Example 3.4.9. A direct symbolic calculation with `Mathematica` shows that

$$s_{27} \equiv 458738443 \bmod 2^{29} - 1$$

and

$$s_{29} \equiv 0 \bmod 2^{31} - 1.$$

Therefore, M_{29} is not prime and M_{31} is a prime. The largest known prime (at the time of this writing: October 2011) is the Mersenne prime

$$2^{43112609} - 1;$$

it has 12978189 digits.

3.5. Some arithmetical properties

Many arithmetic properties of the Fibonacci numbers come directly from the representation given in Theorem 3.3.3. Some of them are discussed next.

Exercise 3.5.1. The sequences of Fibonacci numbers and Lucas numbers satisfy $\gcd(F_n, F_{n+1}) = 1$ and $\gcd(L_n, L_{n+1}) = 1$.

Exercise 3.5.2. Prove that $F_n \equiv L_n \bmod 2$.

Exercise 3.4.4 shows that F_n divides F_{2n}. This result is generalized in the next proposition.

Proposition 3.5.3. *For every* $n, r \in \mathbb{N}$, F_n *divides* F_{rn}.

Proof. The identity (3.4.3) shows that

$$2F_{rn} = F_n L_{(r-1)n} + F_{(r-1)n} L_n \tag{3.5.1}$$

and induction on the index r gives that F_n divides $2F_{rn}$. In the case where F_n is odd, it follows that F_n divides F_{rn}. If F_n is even, Exercise

3.5.2 shows that L_n is also. The term $F_{(r-1)n}$ is divisible by F_n; hence it is even. It follows from this that $L_{(r-1)n}$ is also even. Now write

$$F_{rn} = F_n \cdot \tfrac{1}{2}L_{(r-1)n} + F_{(r-1)n} \cdot \tfrac{1}{2}L_n \tag{3.5.2}$$

to conclude by induction that F_n divides F_{rn}. □

Theorem 3.5.4. *The Fibonacci numbers satisfy*

$$\gcd(F_n, F_m) = F_{\gcd(n,m)}. \tag{3.5.3}$$

Proof. Let $h = \gcd(F_n, F_m)$ and $d = \gcd(n, m)$. There are integers r, s such that $d = rm + sn$. Proposition 3.5.3 shows that h divides F_{rm} and F_{sn}. Exercise 3.4.3 yields

$$F_{rm}L_{sn} + F_{sn}L_{rm} = 2F_{rm+sn} = 2F_d, \tag{3.5.4}$$

and it follows that h divides $2F_d$. In the case where h is odd, it follows that h divides F_d. If h is even, then F_n and F_m are even. Now write (3.5.4) as

$$F_d = F_{rm} \cdot \tfrac{1}{2}L_{sn} + F_{sn} \cdot \tfrac{1}{2}L_{rm} \tag{3.5.5}$$

to conclude that h divides F_d also in this case. To conclude the proof, use Proposition 3.5.3 to see that F_d divides F_n and F_m. Therefore F_d divides $\gcd(F_n, F_m) = h$. □

The previous statement has an unexpected consequence.

Corollary 3.5.5. *There are infinitely many primes.*

Proof. Assume that $p_1, p_2, \ldots, p_k$ is the list of all primes without including 2. Then every element of the list

$$F_{p_1},\, F_{p_2}, \ldots, F_{p_k} \tag{3.5.6}$$

must be divisible by a different prime because $\gcd(F_{p_i}, F_{p_j}) = 1$ for $i \neq j$. The pigeon-hole principle shows that F_{p_k} is divisible by a single prime from the previous list. Therefore F_{p_k} must be of the form $2^a p^b$. But $F_{19} = 13 \cdot 37$ is not of this form. This contradiction establishes the result. □

Divisibilty properties of the Fibonacci numbers are presented next.

• A **Fibonacci prime** is a prime of the form F_n. The indices up to 10000 that produce primes are

$$3, 4, 5, 7, 11, 13, 17, 23, 29, 43, 47, 83, 131, 137, 359,\\ 431, 449, 509, 569, 571, 2971, 4723, 5387, 9311, 9677.$$

It has been conjectured that there are infinitely many Fibonacci primes.

• If $p \neq 5$ is a prime, then p does not divides F_p. On the other hand, there are many indices n for which n divides F_n. The values of $n \leq 500$ for which this holds are

$$1, 5, 12, 24, 25, 36, 48, 60, 72, 96, 108, 120, 125, 144, 168,\\ 180, 192, 216, 240, 288, 300, 324, 336, 360, 384, 432, 480.$$

The data suggests the following statement: if n is odd and n divides F_n, then n is a power of 5. On the other hand, the only indices $n \leq 10^6$ for which n^2 divides F_n are $n = 1$ and $n = 12$ (in both cases $F_n = n^2$).

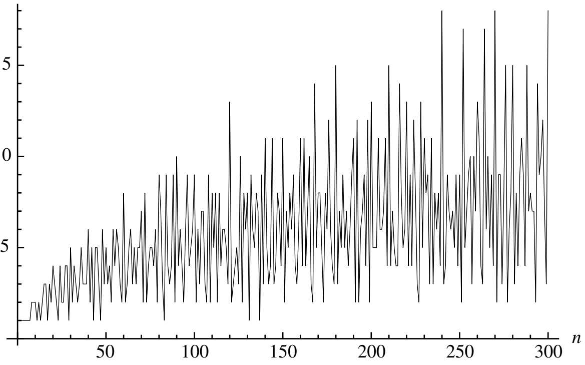


Figure 3.5.1. Number of prime factors of F_n.

• The graph in Figure 3.5.1 shows the number of prime factors of F_n. *Is is possible to make a conjecture on this function?*

• The graphs of the 7-adic valuations of F_n are depicted in Figures 3.5.2 and 3.5.3. The range of n increases in each figure. Observe that the graph has a similar pattern as the valuation of n shown in

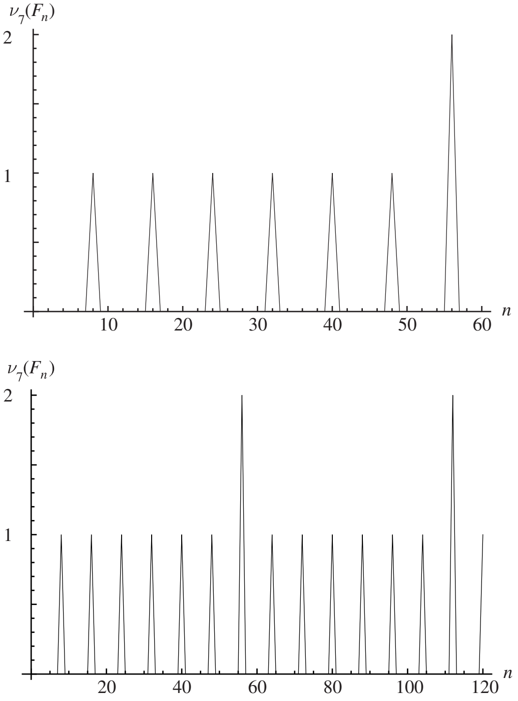


Figure 3.5.2. The 7-adic valuation of Fibonacci numbers.

Figure 1.7.1. In this case, the data begins with a string of six 0's (corresponding to the fact that $\nu_7(n) = 0$ for $1 \leq n \leq 6$) followed by a 1 at position $n = 7$. This is followed by another string of 0's and then a 1 at position 14. The natural tool for describing these patterns is the generating function

$$h_7(x) := \sum_{n=1}^{\infty} \nu_7(n) x^n.$$

The first few terms of this function are given by

$$\begin{aligned} h_7(x) &= x^7 + x^{14} + x^{21} + x^{28} + x^{35} + x^{42} + 2x^{49} \\ &\quad + x^{56} + x^{63} + x^{70} + x^{77} + x^{84} + x^{91} + 2x^{98} + \cdots . \end{aligned}$$

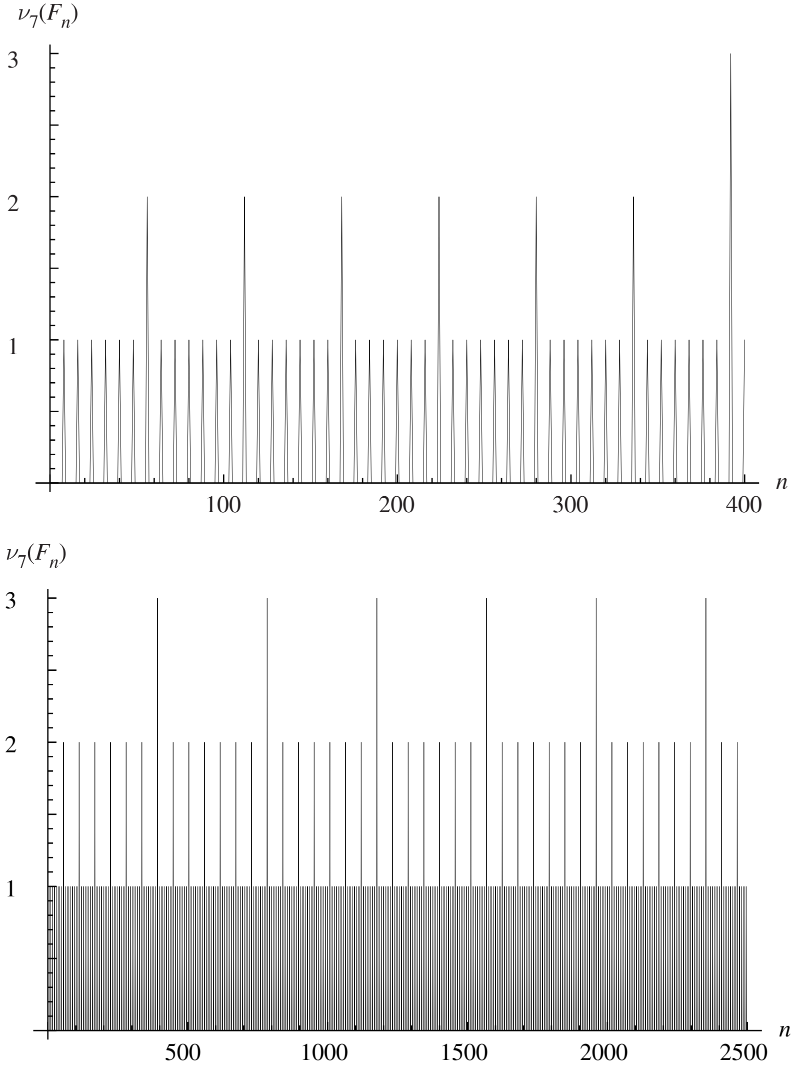


Figure 3.5.3. The 7-adic valuation of Fibonacci numbers.

On the other hand, the generating function

$$f_7(x) := \sum_{n=1}^{\infty} \nu_7(F_n)x^n$$

begins as

$$\begin{aligned} f_7(x) &= x^8 + x^{16} + x^{24} + x^{32} + x^{40} + x^{48} + 2x^{56} \\ &\quad + x^{64} + x^{72} + x^{80} + x^{88} + x^{96} + x^{104} + 2x^{112} + \cdots . \end{aligned}$$

This has the same behavior as $h_7(x)$ but the period is 8 instead of 7.

Definition 3.5.6. The sequence $\{a_n\}$ is called of **type** r if the generating function $a_0 + a_1x + a_2x^2 + \cdots$ is a formal power series in the variable $y = x^r$. This is equivalent to saying that if r does not divide n, then $a_n = 0$.

Exercise 3.5.7. Check that, for any prime p, the sequence $\nu_p(n)$ is of type p.

The table below shows the type of the sequence $\nu_p(F_n)$, denoted by τ_p, as a function of the prime p.

p	3	5	7	11	13	17	19	23	29	31	37	41	43	47
τ_p	4	5	8	10	7	9	18	24	14	30	19	20	44	16

Observe that the data above suggests that τ_p divides $p-1$ or $p+1$ unless $p = 5$. In this last case $\tau_5 = 5$. The special role that the prime $p = 5$ plays with the Fibonacci sequence is illustrated in Theorem 3.5.9. The proof will employ the next exercise.

Exercise 3.5.8. Establish the identity

$$2^{n-1}F_n = \sum_{k=0}^{\infty} \binom{n}{2k+1} 5^k. \tag{3.5.7}$$

Hint: Apply the binomial theorem to

$$F_n = \frac{1}{2^n\sqrt{5}} \left((1+\sqrt{5})^n - (1-\sqrt{5})^n \right). \tag{3.5.8}$$

A second proof may be obtained by computing the generating function of both sides. Exercise 2.11.11 should be useful. A third proof via the WZ-method is outlined next. Let $A(n,k) = \binom{n}{2k+1}5^k$. Use the WZ-method to obtain the companion $B(n,k) = -\binom{n}{2k-1}5^k$ and verify the identity

$$A(n+2,k) - 2A(n+1,k) - 4A(n,k) = B(n,k+1) - B(n,k).$$

Sum this relation over all values of k to produce $a_{n+2} - 2a_{n+1} - 4a_n = 0$, where $a_n := \sum_{k \in \mathbb{Z}} A(n,k)$. Now define $b_n = 2^{n-1}F_n$ and use $F_{n+2} - F_{n+1} - F_n = 0$ to verfiy that b_n satisfies the same recurrence as a_n. Finally check that the initial conditions match.

Theorem 3.5.9. *The* 5*-adic valuation of Fibonacci numbers satisfies* $\nu_5(F_n) = \nu_5(n)$.

Proof. The identity $\binom{n}{2k+1} = \frac{n}{2k+1}\binom{n-1}{2k}$ shows that

$$\begin{aligned}\nu_5\left(\binom{n}{2k+1}5^k\right) &= \nu_5\left(\frac{n}{2k+1}\binom{n-1}{2k}5^k\right) \\ &= \nu_5(n) - \nu_5(2k+1) + \nu_5\left(\binom{n-1}{2k}5^k\right) \\ &\geq \nu_5(n) - \nu_5(2k+1) + k.\end{aligned}$$

This last term is strictly bigger than $\nu_5(n)$, unless $k = 0$. For $k = 0$, it becomes $\nu_5(n)$. The result now follows from Exercise 3.5.8. □

Definition 3.5.10. For a prime p, let α_p be the least index n for which p divides F_n.

Note 3.5.11. Figure 3.5.4 shows the data for primes $2 \leq p \leq 7919$ (this is the 1000th prime). The horizontal axis is x, where p is the xth prime; the vertical axis is α_p.

Exercise 3.5.12. Prove that α_p is well-defined. That is, show that for each prime p there is some n for which p divides F_n. This property actually characterizes Fibonacci numbers among all sequences satisfying $x_n = x_{n-1} + x_{n-2}$ with $x_0 = a$ and $x_1 = b$. The paper by U. Alfred [**6**] contains some details.

Note 3.5.13. T. Lengyel [**199**] has determined analytic expressions for the p-adic valuations of Fibonacci numbers. First

$$\nu_2(F_n) = \begin{cases} 0 & \text{if } n \equiv 1, 2 \bmod 3, \\ 1 & \text{if } n \equiv 3 \bmod 6, \\ 3 & \text{if } n \equiv 6 \bmod 12, \\ \nu_2(n) + 4 & \text{if } n \equiv 0 \bmod 12. \end{cases}$$

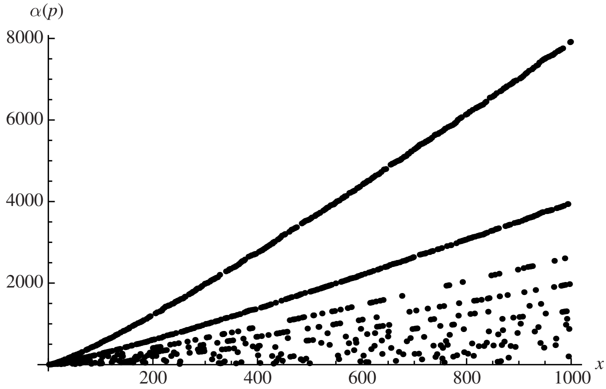


Figure 3.5.4. The smallest n for which p divides F_n.

The expression for $p \neq 2, 5$ employs the number α_p, defined as the first positive integer n where $F_n \equiv 0 \bmod p$. Its existence is established in the next section. Then

$$\nu_p(F_n) = \begin{cases} \nu_p(n) + \nu_p(F_{\alpha_p}) & \text{if } n \equiv 0 \bmod \alpha_p, \\ 0 & \text{otherwise.} \end{cases}$$

Note 3.5.14. A sequence of integers $s(n)$ is called k**-regular** if there exists an integer $d \geq 1$ and integers $c_{i,e,j}$ such that for each $0 \leq i \leq k^d - 1$ the subsequence $s(k^d n + i)$ can be written as a linear combination

$$s(k^d n + i) = \sum_{e=0}^{d-1} \sum_{j=0}^{k^e - 1} c_{i,e,j}\, s(k^e n + j) \tag{3.5.9}$$

of subsequences $s(k^e n + j)$, where $0 \leq e \leq d-1$ and $0 \leq j \leq k^e - 1$. Therefore, in order to compute $s(n)$, start by determining the residue class of n modulo k^d and then use the equation to write $s(n)$ in terms of $s(n')$, with smaller n'.

For example, consider the **Thue-Morse sequence** $t(n)$ defined by

$$t(n) = \begin{cases} 0 & \text{if } s_2(n) \text{ is even}, \\ 1 & \text{if } s_2(n) \text{ is odd}, \end{cases} \tag{3.5.10}$$

where $s_2(n)$ is the number of 1's in the binary representation of n. This sequence starts as

$$0,\ 1,\ 1,\ 0,\ 1,\ 0,\ 0,\ 1,\ 1,\ 0,\ 0,\ 1,\ 0,\ 1,\ 1,\ 0,\ 1,\ 0,\ 0,\ 1,\ 0,\ 1,\ 1. \tag{3.5.11}$$

Considering the binary representation of n, it follows that

$$\begin{aligned} t(4n+0) &= t(n), \\ t(4n+1) &= t(2n+1), \\ t(4n+2) &= t(2n+1), \\ t(4n+3) &= t(n). \end{aligned} \tag{3.5.12}$$

Therefore, $t(n)$ is 2-regular with $d = 2$. The recurrences (3.5.12), along with the initial conditions $t(0) = 0$ and $t(1) = 1$, uniquely determines $t(n)$. The Thue-Morse sequence was independently discovered in several contexts. It has the interesting property of being an infinite sequence on a binary alphabet, which avoids cubes: no block of 0's and 1's occurs three times consecutively.

A recent result of L. Medina and E. Rowland [**215**] states that the sequence $\{\nu_p(F_n) : n \in \mathbb{N}\}$ is k-regular. The value of k has been conjectured to be related to the number α_p defined in Note 3.5.13. Z. Shu and J.-Y. Yai [**272**] have established this result in the context of p-adic analytic functions.

3.6. Modular properties of Fibonacci numbers

Let $r \in \mathbb{N}$ be fixed. In this section the properties of the Fibonacci numbers F_n modulo r are considered. The case $r = 2$ is easy to determine. The parity of F_n leads to the sequence $\{1, 1, 0, 1, 1, 0, \ldots\}$.

Theorem 3.6.1. *The Fibonacci numbers F_n modulo 2 form a periodic sequence of period 3 and repeating pattern $\{1, 1, 0\}$.*

Proof. The first three values are indeed congruent to 1, 1, 0 modulo 2. Now assume that this pattern persists for the first $3n$ numbers. Then $F_{3n+1} = F_{3n} + F_{3n-1} \equiv 0 + 1 = 1 \mod 2$. The residues of F_{3n+2} and F_{3n+3} are obtained by a similar argument. □

The extension of the periodicity is easy to establish.

Theorem 3.6.2. *Let $r \in \mathbb{N}$. The Fibonacci numbers modulo r form a periodic sequence.*

Proof. The total number of possible pairs $(F_i \bmod r, F_{i+1} \bmod r)$ is r^2. Therefore some ordered pair must occur more than once, so pick one that repeats and label it n and $n+j$; that is,

$$(F_n \bmod r,\ F_{n+1} \bmod r) = (F_{n+j} \bmod r,\ F_{n+j+1} \bmod r)\,.$$

Then induction on $k \geq 2$ and using the recurrence for the Fibonacci numbers show that $F_{n+k} \bmod r = F_{n+k+j} \bmod r$. Therefore the sequence $F_n \bmod r$ is periodic. □

Note 3.6.3. This property actually characterizes Fibonacci numbers among all sequences satisfying $x_n = x_{n-1} + x_{n-2}$ with $x_0 = a$ and $x_1 = b$. The paper by U. Alfred [**6**] contains some details.

Definition 3.6.4. The minimal period of the sequence $\{F_n \bmod r\}$ is denoted by $\text{per}(r)$.

Example 3.6.5. The value $\text{per}(2) = 3$ was established already. For $r = 3$ the Fibonacci numbers reduced modulo r start as

$$\{1,\ 1,\ 2,\ 0,\ 2,\ 2,\ 1,\ 0,\ 1,\ 1, \ldots\}. \tag{3.6.1}$$

The repetition of the pair $\{1,\ 1\}$ shows that $\text{per}(3) = 8$.

Exercise 3.6.6. Check that $\text{per}(4) = 6$ and $\text{per}(5) = 20$.

The results described next appeared in the paper by D. D. Wall [**302**]. The first one relates the period $\text{per}(r)$ to the prime factorization of r.

Theorem 3.6.7. *Let $r = p_1^{n_1} p_2^{n_2} \ldots p_s^{n_s}$. Then*

$$\text{per}(r) = \text{lcm}\left\{\text{per}(p_1^{n_1}), \ldots, \text{per}(p_s^{n_s})\right\}. \tag{3.6.2}$$

Therefore, the function per *is determine by its values at powers of prime numbers.*

Proof. For p prime, the sequence $F_n \bmod p^k$ repeats only after blocks of length multiples of $\text{per}(p^k)$. The sequence $F_n \bmod r$ repeats after blocks of length $\text{per}(r)$. In particular, the same is true for $F_n \bmod p_i^{n_i}$. Therefore $\text{per}(r)$ is divisible by the period $\text{per}(p_i^{n_i})$

for each i in the range $1 \leq i \leq s$. It follows that the least common multiple of these periods must divide $\text{per}(r)$. The remainder of the argument is left as the next exercise □

Exercise 3.6.8. Complete the proof of Theorem 3.6.7.

Note 3.6.9. J. Kramer and V. E. Hoggatt Jr. [**188**] show that the period modulo 2^n is $3 \cdot 2^{n-1}$ and modulo 5^n it is $4 \cdot 5^n$.

The sequence $F_n \bmod r$ for $n \geq 0$ always begins with $\{0, 1, 1\}$. The periodicity shows that $F_{\text{per}(r)} \equiv 0 \bmod r$. The next theorem characterizes the indices that produce Fibonacci numbers divisible by r.

Theorem 3.6.10. *Let $r \in \mathbb{N}$. Then there exists $d(r) \in \mathbb{N}$ such that if n satisfies $F_n \equiv 0 \bmod r$, then $n \equiv 0 \bmod d(r)$. That is, all indices n for which F_n is divisible by r are multiples of a fixed number $d(r)$.*

Proof. The proof establishes that the set $\{k \in \mathbb{N} : F_k \equiv 0 \bmod r\}$ is closed under addition and subtraction (provided the result is positive). This gives the statement of the theorem.

Assume $F_i \equiv F_j \equiv 0 \bmod r$. The relation (3.2.4) gives

$$F_{i+j} = F_{i+1}F_j + F_iF_{j-1} \tag{3.6.3}$$

and it follows that $F_{i+j} \equiv 0 \bmod r$. To check the result about differences, assume $i > j$ and take $n = j$ and $m = i - j$ in (3.2.4). This yields

$$F_i = F_{j+1}F_{i-j} + F_jF_{i-j-1}. \tag{3.6.4}$$

Conclude that

$$F_{j+1}F_{i-j} \equiv 0 \bmod r. \tag{3.6.5}$$

Let p be a prime that divides $\gcd(F_{j+1}, r)$. The condition $F_j \equiv 0 \bmod r$ implies p divides F_j. Therefore p divides $\gcd(F_{j+1}, F_j) = 1$. This contradiction shows that F_{j+1} is relatively prime to r and (3.6.5) now gives $F_{i-j} \equiv 0 \bmod r$, as claimed. □

Corollary 3.6.11. *Let $r \in \mathbb{N}$. Then $d(r)$ divides* $\text{per}(r)$.

The paper by D. D. Wall [**302**] cited earlier also contains a proof of the next result.

Theorem 3.6.12. *Let p be a prime. If* $\mathrm{per}(p) \neq \mathrm{per}(p^2)$*, then* $\mathrm{per}(p^k) = p^{k-1}\mathrm{per}(p)$ *for* $k \geq 2$*.*

Note 3.6.13. There are no reported values where $\mathrm{per}(p) = \mathrm{per}(p^2)$ occurs. This question is similar to the one for Fermat quotient described in Note 2.5.12.

Exercise 3.6.14. Construct a table with the values $\mathrm{per}(p^k)$.

3.7. Continued fractions of powers of Fibonacci quotients

The reader who has solved Exercise 3.3.7 has observed the pattern

$$\frac{F_6}{F_5} = \frac{8}{5} = 1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1}}}}.$$

The observation described in this section came from a simple computer experiment. What is the structure of the continued fraction of powers of the quotient F_{n+1}/F_n? The result is surprising and it shows one more time the intimate relation between the number 5 and the Fibonacci numbers.

Exercise 3.7.1. Prove that the continued fraction of the golden ratio φ is $\varphi = [1, 1, 1, 1, \ldots]$. Check that the convergents of φ are F_{n+1}/F_n.

The continued fraction of $(F_{n+1}/F_n)^2$ has similar features to that of F_{n+1}/F_n. For example,

$$\left(\frac{F_{16}}{F_{15}}\right)^2 = [2, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 3, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1].$$

An unexpectedly large partial quotient appeared in

$$\left(\frac{F_{16}}{F_{15}}\right)^5 = [11, 11, 10, 2, 269253, 18, 11, 10, 1, 4, 11, 11],$$

but no large partial quotient appears for other powers. The following table shows the *number of digits* of the maximum partial quotient appearing in the continued fraction of $(F_{n+1}/F_n)^a$, for $1 \leq n \leq 5000$, as a function of the exponent a. In the table, this function is denoted by $\omega(a)$:

a	1	2	3	4	5	6	7	8	9	10
$\omega(a)$	1	1	2	2	2090	4	5	7	7	8

a	11	12	13	14	15	16	17	18	19	20
$\omega(a)$	9	9	9	9	8	10	9	8	8	8

The value of $\omega(5)$ becomes 4180 if the range of n is increased to $n \leq 10000$.

The explanation of part of this phenomenon is provided by the next result. The author wishes to thank J. Shallit for this information. The actual proof, not presented here, is due to H. Cohn [**102**].

Theorem 3.7.2. *A continued fraction of* $(F_{5n+1}/F_{5n})^5$ *is*

$$[11^{[n-1]}, 10, 1, 1, \alpha, 1, 17, 11^{[n-2]}, 10, 1, 4, 11^{[n-1]}],$$

where $\alpha = (-1)^n \frac{1}{5}(4F_{5n}^2 - F_{5n-1}^2 + 4(-1)^{n+1})$. *In particular, the largest partial quotient is* $|\alpha|$. *Here* $11^{[j]}$ *is meant to be a sequence of* 11*'s of length* j. *Note that the term* α *could be negative, so this is not the canonical continued fraction.*

3.8. Fibonacci polynomials

The recurrence defining the Fibonacci numbers is now extended by the introduction of a parameter x. The new numbers now depend on x and are defined by

$$F_n(x) = xF_{n-1}(x) + F_{n-2}(x) \tag{3.8.1}$$

with the initial conditions $F_0(x) = 0$ and $F_1(x) = 1$.

It is clear that $F_n(x)$ is a polynomial in x of degree $n-1$. It is called the **Fibonacci polynomial**. Observe that $F_n(1) = F_n$, the Fibonacci number.

An extension of Theorem 3.3.3 is presented next.

Theorem 3.8.1. *Let* $\alpha = (x+\sqrt{x^2+4})/2$ *and* $\beta = (x-\sqrt{x^2+4})/2$. *Then*

$$F_n(x) = \frac{\alpha^n - \beta^n}{\alpha - \beta}.$$

Proof. Solve the recurrence (3.8.1) as indicated in Exercise 3.2.1. □

Exercise 3.8.2. Use the recurrence (3.8.1) to establish the formula

$$F_n(x) = \sum_{j=0}^{\lfloor \frac{n-1}{2} \rfloor} \binom{n-j-1}{j} x^{n-2j-1}. \tag{3.8.2}$$

3.8.1. The zeros of Fibonacci polynomials.

Given a family of polynomials, such as $\{F_n(x) : n \in \mathbb{N}\}$, it is very unusual that the zeros can be computed explicitly. This can be done for the Fibonacci family. The result is due to V. E. Hoggart Jr. [**175**]. The argument employs elementary properties of the hyperbolic functions.

The change of variables $x = 2i \cosh z$ gives $\sqrt{x^2+4} = 2i \sinh z$ and also $\alpha = ie^z$, $\beta = ie^{-z}$. Therefore,

$$F_n(x) = i^{n-1} \frac{\sinh nz}{\sinh z}.$$

The computation of the zeros of F_n can be done explicitly. The result is stated below.

Theorem 3.8.3. *The zeros of the Fibonacci polynomial $F_n(x)$ are given by*

$$x_k = 2i \cos \frac{\pi k}{n}, \qquad \textit{for } 1 \leq k \leq n-1.$$

3.8.2. Some integrals containing Fibonacci polynomials.

The explicit expression for the zeros of Fibonacci polynomials provides a closed-form formula for certain definite integrals. The next exercise appears in [**269**] as a problem proposed by H. J. Seiffert and solved by P. S. Bruckman.

Exercise 3.8.4. Show that for even $n \geq 4$

$$\int_{-\infty}^{\infty} \frac{dx}{F_n(x)} = \frac{\pi}{n} \left(1 + \frac{1}{\cos \pi/n} \right)$$

and for odd $n \geq 3$

$$\int_{-\infty}^{\infty} \frac{x\,dx}{F_n(x)} = \frac{\pi}{n} \left(\tan \frac{\pi}{2n} + \tan \frac{3\pi}{2n} \right).$$

On the other hand, the explicit formula (3.8.2) may be used to evaluate integrals involving Fibonacci polynomials. Two examples are presented here.

Example 3.8.5. Consider the integral

$$e_n := \int_0^\infty F_n(x) e^{-x} dx. \tag{3.8.3}$$

Then (3.8.2) yields

$$e_n = \sum_{j=0}^{\lfloor \frac{n-1}{2} \rfloor} \frac{(n-j-1)!}{j!}. \tag{3.8.4}$$

Exercise 3.8.6. Confirm that e_n is a positive integer.

The p-adic valuations of the sequence e_n seem to follow some regular patterns. Here is an experimental observation:

- For the prime $p = 2$ the data indicates that $\nu_2(e_n) = 0$ if $n \not\equiv 0 \bmod 4$ and

$$\nu_2(e_{4n}) = \nu_2(n) + \begin{cases} 3 & \text{if } n \equiv 1 \bmod 2, \\ 5 & \text{if } n \equiv 2 \bmod 4, \\ 6 & \text{if } n \equiv 0 \bmod 4. \end{cases}$$

- For the prime $p = 3$, it seems that $\nu_3(e_n) = 0$ if $n \not\equiv 0 \bmod 3$ and $\nu_3(e_{3n}) = 1$ if $n \not\equiv 0 \bmod 6$. The remaining case is given by $\nu_3(e_{18n}) = \nu_3(n) + 2$.

Exercise 3.8.7. Develop a systematic procedure to find the $\nu_p(e_n)$ and prove them. **Warning:** The author has not tried to do this.

Example 3.8.8. The second family of integrals corresponds to

$$g_n := \int_0^\infty F_n(x) e^{-x^2}\, dx. \tag{3.8.5}$$

This also has interesting arithmetic patterns. The first few values are

$$\frac{\sqrt{\pi}}{2}, \frac{1}{2}, \frac{3\sqrt{\pi}}{2}, \frac{3}{2}, \frac{13\sqrt{\pi}}{8}, \frac{9}{2}, \frac{77\sqrt{\pi}}{16}, 16.$$

Then (3.8.2) gives

$$g_n = \sum_{j=0}^{\lfloor \frac{n-1}{2} \rfloor} \binom{n-j-1}{j} \int_0^\infty x^{n-2j-1} e^{-x^2}\, dx. \tag{3.8.6}$$

The integrals appearing in the sum may be evaluated either by producing recurrences for them or by employing the gamma function described in Chapter 16. The next exercise outlines the evaluation by recurrences.

Exercise 3.8.9. Let

$$J_n = \int_0^\infty x^n e^{-x^2}\, dx. \tag{3.8.7}$$

Establish the recurrence

$$J_n = \frac{n-1}{2} J_{n-2}. \tag{3.8.8}$$

Compute the initial conditions $J_0 = \sqrt{\pi}/2$ and $J_1 = 1/2$ and use them to verify the formulas

$$\int_0^\infty x^n e^{-x^2}\, dx = \frac{1}{2}\left(\frac{n-1}{2}\right)! \quad \text{if } n \text{ is odd} \tag{3.8.9}$$

and

$$\int_0^\infty x^n e^{-x^2}\, dx = \frac{\sqrt{\pi}}{2^{n+1}} \frac{n!}{(n/2)!} \quad \text{if } n \text{ is even.} \tag{3.8.10}$$

This result is now employed to produce an expression for g_n.

Theorem 3.8.10. *The integral g_n is given according to parity by*

$$g_{2n} = \frac{1}{2} \sum_{k=0}^{n-1} \binom{n+k}{2k+1} k!$$

and

$$g_{2n+1} = \frac{\sqrt{\pi}}{2} \sum_{k=0}^{n} \binom{n+k}{2k} \binom{2k}{k} \frac{k!}{2^{2k}}.$$

Proof. The definition of g_n gives

$$g_n = \sum_{j=0}^{\left\lfloor \frac{n-1}{2} \right\rfloor} \binom{n-j-1}{j} \int_0^\infty x^{n-2j-1} e^{-x^2}\, dx. \tag{3.8.11}$$

The result now follows from Exercise 3.8.9. □

This pattern suggests considering the indices according to their parity. Define

$$g_n' = \begin{cases} g_n/\sqrt{\pi} & \text{if } n \text{ is odd,} \\ g_n & \text{if } n \text{ is even.} \end{cases} \tag{3.8.12}$$

Then the modified sequence g_n' starts as

$$\frac{1}{2},\ \frac{1}{2},\ \frac{3}{4},\ \frac{3}{2},\ \frac{13}{8},\ \frac{9}{2},\ \frac{77}{16},\ 16,\ \frac{591}{32},\ \frac{139}{2},\quad 1 \leq n \leq 10. \tag{3.8.13}$$

Exercise 3.8.11. Prove that the denominators of g_n' are always a power of 2; denote this power by $2^{R(n)}$. Prove $R(2n-1) = n$. In the case of even indices, prove that $i \equiv j \bmod 4$ implies $R(i) = R(j)$ and

$$R(2n) = \begin{cases} 1 & \text{if } n \not\equiv 0 \bmod 8, \\ 0 & \text{if } n \equiv 0 \bmod 8. \end{cases}$$

Now define

$$y_n = 2g_{8n} = \sum_{k=0}^{4n-1} \binom{4n+k}{2k+1} k! \tag{3.8.14}$$

and produce experimental evidence of

$$\nu_2(y_n) = \begin{cases} 5 & \text{if } n \text{ is odd}, \\ 3 + \nu_2(n) & \text{if } n \text{ is even}. \end{cases} \tag{3.8.15}$$

Note 3.8.12. The valuation tree for the sequence $\nu_3(y_n)$ is described next. The reader will find information about the construction of a valuation tree in Note 1.7.3. In the present case, the splitting parameter is 3; that is, at each level, an unlabeled vertex produces 3 descendents.

The beginning of the process is depicted in Figure 3.8.1.

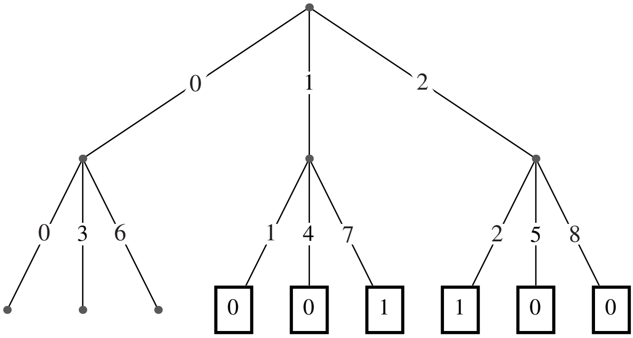


Figure 3.8.1. The 3-adic valuation of the sum y_n.

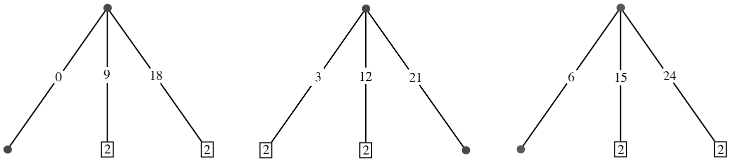


Figure 3.8.2. The 3-adic valuation of the sum y_n (continuation).

The first level corresponds to the three classes modulo 3. There are no labeled vertices at this level because none of the classes have constant 3-adic valuation. The second level corresponds to classes modulo $3^2 = 9$. The splitting parameter for this problem is 3. There are now six classes that have been labeled, corresponding to classes that have constant valuation. For instance $\nu_3(y_{9n+7}) = 1$.

The three nodes of the second level that remain unlabeled correspond to the modular classes $n \equiv 0 \bmod 9$, $n \equiv 3 \bmod 9$, and $n \equiv 6 \bmod 9$. The continuation of the valuation tree is shown in Figure 3.8.2. These trees have to be attached to the left branch of the tree shown in Figure 3.8.1. Each vertex in these classes is now split again into three new vertices. These (nine) vertices form the next level. The process is repeated. For instance, the class $n \equiv 3 \bmod 9$ is split into $n \equiv 3 \bmod 27$, $n \equiv 12 \bmod 27$, and $n \equiv 21 \bmod 27$. The last two have constant 3-adic valuation and they have been labeled. The first one has to be split again, to produce nine new vertices. It is temping to state the following:

Conjecture 3.8.13. *In each level of the valuation tree for y_n, there are three unlabeled nodes.*

3.9. Series involving Fibonacci numbers

The literature contains a variety of series whose general term involves the Fibonacci numbers. A couple of examples are presented here.

Example 3.9.1. The most elementary examples come from the generating function (3.3.2). For instance, taking $x = 1/k$ leads to

$$\sum_{n=0}^{\infty} \frac{F_n}{k^n} = \frac{k}{k^2 - k - 1}.$$

The special case of $k = 10$ gives the *decimal-looking expansion*

$$\sum_{n=0}^{\infty} \frac{F_n}{10^n} = \frac{10}{89}.$$

This is not quite a decimal expansion because $F_n > 9$ for $n \geq 7$.

Exercise 3.9.2. Prove that

$$\sum_{n=1}^{\infty} \frac{nF_n}{2^n} = 10.$$

Define

$$N_r = \sum_{n=1}^{\infty} \frac{n^r F_n}{2^n}.$$

Compute the first few values and then prove that $\nu_2(N_r) = 1$; that is, $\frac{1}{2}N_r$ is an odd number.

Example 3.9.3. The second example may be found in the paper by I. J. Good [**139**]. The presentation begins with a couple of exercises.

Exercise 3.9.4. Let F_n, L_n be the Fibonacci and Lucas numbers, respectively. Prove the identity

$$L_{2^n}F_{2^n-1} - 1 = F_{2^{n+1}-1}.$$

Hint: Use (3.3.10) and (3.4.2) to reduce the question to a statement about the roots $\varphi_{\pm}$. Then use $\varphi_{+}\varphi_{-} = -1$.

Exercise 3.9.5. Prove the identity

$$\sum_{j=0}^{n} \frac{1}{F_{2^j}} = 3 - \frac{F_{2^n-1}}{F_{2^n}}.$$

A combinatorial proof of this identity has been given by N. Shar [**271**].

The second series is known as the **Millin series**:

$$\sum_{j=0}^{\infty} \frac{1}{F_{2^j}} = \frac{7-\sqrt{5}}{2}. \tag{3.9.1}$$

It is obtained by letting $n \to \infty$ in Exercise 3.9.5 and using

$$\lim_{n\to\infty} \frac{F_{n-1}}{F_n} = \varphi_{+} = \frac{\sqrt{5}-1}{2}.$$

This example was generalized by W. E. Greig [**149**] to

$$\sum_{j=0}^{n} \frac{1}{F_{k2^j}} = g_k - \frac{F_{k2^n-1}}{F_{k2^n}},$$

where

$$g_k = \begin{cases} \frac{1+F_{k-1}}{F_k} & \text{if } k \text{ is even,} \\ \frac{1+F_{k-1}}{F_k} + \frac{2}{F_{2k}} & \text{if } k \text{ is odd.} \end{cases}$$

This leads to

$$\sum_{j=0}^{\infty} \frac{1}{F_{k2^j}} = g_k - \frac{\sqrt{5}-1}{2}. \tag{3.9.2}$$

Note 3.9.6. Other examples appearing in the literature include

$$\sum_{k=0}^{\infty} \frac{1}{1+F_{2k+1}} = \frac{\sqrt{5}}{2} \quad \text{and} \quad \sum_{k=0}^{\infty} \frac{1}{3/\sqrt{5}+F_{2k+1}} = 1,$$

a series involving products of Fibonacci numbers

$$\sum_{n=1}^{\infty} \frac{(-1)^{n+1}}{F_n F_{n+1}} = \frac{\sqrt{5}-1}{2},$$

and the remarkable series

$$\sum_{k=1}^{\infty} \frac{(-1)^{k+1}}{\sum_{j=1}^{k} F_j^2} = \frac{\sqrt{5}-1}{2}.$$

Many other series involving Fibonacci numbers are evaluated in terms of the so-called **theta functions**. For instance

$$\sum_{n=1}^{\infty} \frac{1}{F_{2n+1}} = \frac{\sqrt{5}}{4} \vartheta_2^2(\varphi^{-2}),$$

where $\varphi = (\sqrt{5}+1)/2$ is the golden ratio and

$$\vartheta_2(q) = \sum_{n=-\infty}^{\infty} q^{(n+1/2)^2}$$

is one of **Jacobi's theta functions**. Information about these remarkable functions can be found in the book by J. M. Borwein and P. B. Borwein [**71**] that centers around the **arithmetic-geometric**

mean, in the book by H. McKean and V. Moll [**213**], and in the classic book by E. T. Whittaker and G. N. Watson [**311**]. The application to these Fibonacci series is described in Section 3.7 of [**71**].

Note 3.9.7. The question of the irrationality of these type of series has also been explored. The **reciprocal Fibonacci series**

$$\sum_{n=0}^{\infty} \frac{1}{F_n}$$

has been shown to be irrational by R. Andre-Jeannin [**16**]. The reader will find more information on this topic in [**71**].

Chapter 4

Polynomials

4.1. Introduction

Polynomials are among the simplest functions encountered in elementary courses. This chapter describes some examples that will appear throughout the book. Special emphasis is placed on properties of roots of polynomials and combinatorial interpretations of the coefficients.

Definition 4.1.1. A **polynomial** is a function of the form

$$P(x) = \sum_{k=0}^{n} a_k x^k, \quad \text{with } a_n \neq 0. \tag{4.1.1}$$

The numbers a_k are called the **coefficients** of P. The symbol x is called the **variable** of the polynomial P. In the case of $P \neq 0$, the number $n \in \mathbb{N}$ in (4.1.1) is its **degree**. The function $P \equiv 0$ is also declared a polynomial and its degree is $-\infty$.

In this text, the coefficients of the polynomial P are either considered as **parameters** or as elements of one of the number systems described in Chapter 1. The polynomial is assigned the name of the system containing its coefficients. For example, a **complex polynomial** is a polynomial with coefficients in $\mathbb{C}$.

Examples of polynomials include the Fibonacci polynomials that have appeared in Section 3.8. A sample of some other types are presented below.

4.2. Examples of polynomials

Bernoulli polynomials: The evaluation of some finite sums. The value of the sums

$$S_1(n) := 1 + 2 + \cdots + (n-1) + n = \frac{n(n+1)}{2} \tag{4.2.1}$$

and

$$S_2(n) := 1^2 + 2^2 + \cdots + (n-1)^2 + n^2 = \frac{n(n+1)(2n+1)}{6} \tag{4.2.2}$$

can be easily verified. The reader is surely aware of the story of Carl F. Gauss who was requested by his teacher to evaluate (4.2.1) for $n = 100$, an early example of *busy work* employed to keep students quiet. In a short time, the young Carl gives the value 5050, obtained by reversing the order of the terms, writing the sum as

$$S_1(n) = n + (n-1) + (n-2) + \cdots + 2 + 1, \tag{4.2.3}$$

followed by the observation that each vertical addition has the value $n+1$. He concluded that

$$2S_1(n) = n(n+1) \tag{4.2.4}$$

and (4.2.1) follows.

A sequence of polynomials introduced now yields the direct evaluation of the sums discussed above. It turns out to be convenient to change the upper limit of summation and to define

$$S_a(n) := \sum_{k=1}^{n-1} k^a, \qquad \text{for } a \in \mathbb{N}_0 \text{ and } n \in \mathbb{N}, \tag{4.2.5}$$

for $n > 1$ and $S_a(1) = 0$. For example

$$S_0(n) = n - 1 \quad \text{and} \quad S_1(n) = \tfrac{1}{2}n^2 - \tfrac{1}{2}n. \tag{4.2.6}$$

Theorem 4.2.1. *For $a \in \mathbb{N}$, the function $S_a(n)$ is a polynomial in n of degree $a+1$.*

Proof. The proof is based on a recurrence for $S_a(n)$. The identity

$$(k+1)^{a+1} - k^{a+1} = \sum_{j=0}^{a} \binom{a+1}{j} k^j \tag{4.2.7}$$

is summed from $k = 1$ to $n-1$. This produces

$$n^{a+1} - 1 = \sum_{j=0}^{a} \binom{a+1}{j} S_j(n), \tag{4.2.8}$$

so that

$$\binom{a+1}{a} S_a(n) = n^{a+1} - 1 - \sum_{j=0}^{a-1} \binom{a+1}{j} S_j(n). \tag{4.2.9}$$

To prove the result by induction, observe that the sum on the right-hand side of (4.2.9) is a polynomial of degree at most a. Therefore the term n^{a+1} gives the exact degree for S_a. □

Note 4.2.2. The proof above shows that the leading coefficient of $S_a(n)$ is $1/(a+1)$.

Note 4.2.3. The relation (4.2.9) provides a way to compute the polynomials $S_a(n)$ recursively.

Definition 4.2.4. The **Bernoulli polynomial** $B_a(n)$ is defined by $B_a(n) = aS_{a-1}(n) + B_a$. The **Bernoulli number** $B_a = B_a(0)$ is defined by the normalization

$$\int_0^1 B_a(x)\,dx = 0. \tag{4.2.10}$$

An alternative definition, based on generating functions, is given in Chapter 13. For example, for $a = 2$, the recurrence (4.2.9) gives

$$3S_2(n) = n^3 - 1 - (n-1) - \tfrac{3}{2}(n^2 - n), \tag{4.2.11}$$

which produces

$$S_2(n) = \tfrac{1}{3}n^3 - \tfrac{1}{2}n^2 + \tfrac{1}{6}n. \tag{4.2.12}$$

Then

$$B_3(n) = 3S_2(n) + B_3 = n^3 - \tfrac{3}{2}n^2 + \tfrac{1}{2}n + B_3. \tag{4.2.13}$$

The normalization (4.2.10) gives $B_3 = 0$ and the Bernoulli polynomial $B_3(n)$ is given by

$$B_3(n) = n^3 - \tfrac{3}{2}n^2 + \tfrac{1}{2}n. \tag{4.2.14}$$

Exercise 4.2.5. Check that

$$B_4(n) = n^4 - 2n^3 + n^2 - \tfrac{1}{30} \text{ and } B_5(n) = n^5 - \tfrac{5}{2}n^4 + \tfrac{5}{3}n^3 - \tfrac{1}{6}n. \tag{4.2.15}$$

Note 4.2.6. The fact that S_a is a polynomial shows that, for fixed $a \in \mathbb{N}$, the explicit evaluation of $S_a(n)$ is reduced to a **finite computation**. For example, the sum $S_4(n)$ is a polynomial of degree 5 that is determined uniquely from the values

$$\begin{aligned} S_4(1) &= 0, & S_4(2) &= 1, & S_4(3) &= 17, \\ S_4(4) &= 98, & S_4(5) &= 354, & S_4(6) &= 979. \end{aligned}$$

Let $P(x)$ be the unique polynomial of degree 5 that matches the data above. The **interpolating polynomial** given in the next exercise shows how to compute P, producing the result

$$S_4(n) = \sum_{k=1}^{n-1} k^4 = \frac{1}{30}(n-1)n(2n-1)(3n^2-3n-1).$$

This gives $B_5(n)$.

Exercise 4.2.7. Given m points $\{(x_1, y_1), (x_2, y_2), \ldots, (x_m, y_m)\}$, with $x_i \neq x_j$ for $i \neq j$, prove there is a unique polynomial J of degree $m-1$ such that $J(x_i) = y_i$. The explicit formula

$$J(x) = \sum_{i=1}^{m} y_i \prod_{j \neq i} \frac{x - x_j}{x_i - x_j} \tag{4.2.16}$$

was given by J. L. Lagrange.

Eulerian polynomials: The generating function for k^n. The next example is constructed from the generating function for powers

$$Q_n(x) = \sum_{k=1}^{\infty} k^n x^k. \tag{4.2.17}$$

An expression for Q_n is now derived from the geometric series

$$\sum_{k=0}^{\infty} x^k = \frac{1}{1-x}. \tag{4.2.18}$$

Differentiation produces

$$\sum_{k=1}^{\infty} k x^{k-1} = \frac{1}{(1-x)^2}. \tag{4.2.19}$$

To recover the exponent x^k in (4.2.19), multiply the identity by x. This is equivalent to applying the **Euler operator**

$$\vartheta := x\frac{\partial}{\partial x} \tag{4.2.20}$$

to (4.2.18). Therefore,

$$Q_1(x) = \vartheta \frac{1}{1-x} = \frac{x}{(1-x)^2}.$$

Iterating this procedure shows that

$$Q_n(x) = \vartheta^n \frac{1}{1-x}. \tag{4.2.21}$$

The next two examples are

$$Q_2(x) = \frac{x(x+1)}{(1-x)^3} \quad \text{and} \quad Q_3(x) = \frac{x(x^2+4x+1)}{(1-x)^4}$$

and this suggests the following definition:

$$A_n(x) = (1-x)^{n+1}\vartheta^n \frac{1}{1-x}. \tag{4.2.22}$$

The function $Q_n(x)$ is then

$$Q_n(x) = \frac{A_n(x)}{(1-x)^{n+1}}. \tag{4.2.23}$$

The next theorem shows that $A_n(x)$ is a polynomial in x, called the **Eulerian polynomial** of order n.

Theorem 4.2.8. *The function $A_n(x)$ satisfies*

$$A_n(x) = nxA_{n-1}(x) + x(1-x)A_{n-1}'(x), \tag{4.2.24}$$

for $n \geq 1$, with initial value $A_0(x) = 1$. In particular, $A_n(x)$ is a polynomial of degree n with integer coefficients and $A_n(0) = 0$ for $n > 0$.

Proof. Observe that

$$\begin{aligned}(1-x)^{-n-2}A_{n+1}(x) &= \vartheta^{n+1}\frac{1}{1-x} \\ &= \vartheta\left[\vartheta^{n}\frac{1}{1-x}\right] \\ &= \vartheta\left[(1-x)^{-n-1}A_n(x)\right].\end{aligned}$$

The result follows by applying ϑ. □

Note 4.2.9. The **Eulerian numbers** $A_{n,k}$ are defined by

$$A_n(x) = x\sum_{k=0}^{n-1} A_{n,k}x^k. \tag{4.2.25}$$

The numbers $A_{n,k}$ have interesting combinatorial interpretations, similar to those of the **Stirling numbers** described in Chapter 7.

Legendre polynomials: The notion of orthogonality. Given a collection of polynomials

$$\mathfrak{C} = \{r_0(x),\, r_1(x), \ldots, r_n(x)\} \tag{4.2.26}$$

such that the degree of r_i is i, every polynomial P of degree at most n can be expressed in a unique form as

$$P(x) = C_0r_0(x) + C_1r_1(x) + \cdots + C_nr_n(x). \tag{4.2.27}$$

The coefficients C_i can be obtained by matching terms of the same degree: the leading order term yields the equation

$$\text{coefficient of } x^n \text{ in } P = C_n \times \text{ coefficient of } x^n \text{ in } r_n,$$

which determines C_n. Repeating this procedure on the modified equation

$$P(x) - C_nr_n(x) = C_0r_0(x) + C_1r_1(x) + \cdots + C_{n-1}r_{n-1}(x)$$

determines C_{n-1}. This method gives all the coeffients C_i in (4.2.27).

The calculation of the coefficients C_i can be simplified if the polynomials r_i are **orthogonal with respect to a weight function** $w(x)$, in the sense that

$$\int_a^b r_i(x)r_j(x)w(x)\,dx = 0 \quad \text{if } i \neq j.$$

The polynomials are called **orthonormal** if the extra condition

$$\int_a^b r_i^2(x)w(x)\,dx = 1 \tag{4.2.28}$$

is imposed. To determine the coefficient C_i, simply multiply (4.2.27) by $r_i w(x)$ and integrate from a to b to obtain

$$C_i = \int_a^b P(x)r_i(x)w(x)\,dx. \tag{4.2.29}$$

Many interesting families of polynomials appear in this form. The **Legendre polynomials** $P_n(x)$ are orthogonal on $[-1,1]$ with weight function $w(x) \equiv 1$. The choice of weight $w(x) = 1/\sqrt{1-x^2}$ on the interval $[-1,1]$ produces the **Chebyshev polynomials**. The third example considered in this book, the **Hermite polynomials**, are orthogonal on $\mathbb{R}$, with weight $e^{-x^2/2}$. Details are given in Chapter 14.

4.3. The division algorithm

The division algorithm for integers, given as Exercise 1.5.1, was employed in Chapter 1 to discuss arithmetical properties of integers. An extension to the class of polynomials is presented here.

The algorithm is stated for polynomials over those number systems described in Chapter 1 where every nonzero element has an inverse (these systems are called **fields**).

Therefore, the coefficients are assumed to be in $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, or $\mathbb{Z}_p$. The symbol $\mathbb{K}$ will denote one of these sets. The reader should be aware that some results are not valid if, for instance, these fields are replaced by $\mathbb{Z}_p$, the finite field with p elements. More general situations are possible. The reader can find them in the textbooks by M. Artin [**31**] and by J. Schrek [**268**].

Definition 4.3.1. The set of polynomials with coefficients in $\mathbb{K}$ is denoted by $\mathbb{K}[x]$.

The next result is known as the **division algorithm** for $\mathbb{K}[x]$.

Theorem 4.3.2. *Let A, $B \in \mathbb{K}[x]$ with $B \neq 0$. Then there are unique polynomials in $\mathbb{K}[x]$, with $R = 0$ or $\deg(R) < \deg(B)$, such that*

$$A(x) = B(x)Q(x) + R(x). \tag{4.3.1}$$

Proof. The proof is by induction on the degree of A. If $\deg(A) < \deg(B)$, take $Q = 0$ and $R = A$. Otherwise, let

$$A(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \tag{4.3.2}$$

and

$$B(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_0 \tag{4.3.3}$$

with $n \geq m$. Then

$$A(x) - \frac{a_n}{b_m}x^{n-m}B(x)$$

is a polynomial of degree strictly less than $\deg(A)$. Induction gives

$$A(x) - \frac{a_n}{b_m}x^{n-m}B(x) = Q_1(x)B(x) + R_1(x)$$

and

$$A(x) = \left(\frac{a_n}{b_m}x^{n-m} + Q_1(x)\right)B(x) + R_1(x)$$

has the stated form. This proves the existence of polynomials Q and R. Uniqueness is left as an exercise to the reader. □

Exercise 4.3.3. Prove that the polynomials Q and R in Theorem 4.3.2 are uniquely determined by A and B.

Corollary 4.3.4. *Let $A \in \mathbb{K}[x]$ and $x_0 \in \mathbb{K}$. Then*

$$A(x) = Q(x)(x - x_0) + A(x_0). \tag{4.3.4}$$

Proof. Apply the division algorithm to $A(x)$ and $B(x) = x - x_0$. The remainder is either 0 or a polynomial of degree 0, that is, constant. This constant is obtained by evaluating at $x = x_0$. □

Exercise 4.3.5. Discuss an algorithm to find the greatest common divisor of two polynomials based on the division algorithm.

4.4. Roots of polynomials

The evaluation of the polynomial

$$A(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n \tag{4.4.1}$$

at $x_0 \in \mathbb{K}$ only requires additions and multiplications. Therefore $A(x_0) \in \mathbb{K}$. The numbers that yield value 0, called the **roots** of A, are of particular interest. This section describes some of their elementary properties. The central question of how to express the roots of a polynomial in terms of its coefficients is postponed until Section 4.6. There is a large body of knowledge dealing with properties of roots of polynomials. The author is sure that the reader will enjoy browsing the book by P. Borwein [**72**] and the spectacular color figures on P. Borwein's website

`http://www.cecm.sfu.ca/~pborwein`.

The division algorithm gives an upper bound on the number of roots.

Proposition 4.4.1. *The number of roots of a nonzero polynomial* $A \in \mathbb{K}[x]$ *is at most its degree.*

Proof. The proof is by induction on the degree of A. If x_0 is a root of A, the factorization

$$A(x) = (x - x_0)Q(x) \tag{4.4.2}$$

shows that $\deg(Q) = \deg(A) - 1$ and the result follows by induction. □

Note 4.4.2. The example $A(x) = x^2 + 1$ as a polynomial over $\mathbb{R}$ shows that the number of roots could be strictly less than its degree.

Exercise 4.4.3. The result is not true if the coefficients of A are elements of other number systems. For example, the polynomial $A(x) = x^2 - 1$ has four roots in $\mathbb{Z}_8$. Explain where the proof of Proposition 4.4.1 breaks down.

Exercise 4.4.4. Let A, $B \in \mathbb{K}[x]$ and suppose $A(x_i) = B(x_i)$ for $1 \leq i \leq m$ with $m > \max(\text{deg}A, \text{deg}B)$. Prove that $A = B$.

Note 4.4.5. Theorem 4.2.1 states that

$$S_a(n) = \sum_{k=1}^{n-1} k^a \tag{4.4.3}$$

is a polynomial of degree $a + 1$. For fixed $a \in \mathbb{N}$, the previous exercise shows that the expression for S_a can be obtained by a finite computation. For example, to prove the identity

$$S_1(n) = \sum_{k=1}^{n} k = \frac{n(n+1)}{2}, \tag{4.4.4}$$

discussed in Section 1.1, it suffices to verify (4.4.4) for three values, say $n = 1$, 2, and 3. The exercise then shows that the identity is valid for all values of n.

Exercise 4.4.6. Give a proof of

$$S_2(n) = \sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}, \tag{4.4.5}$$

in the same style. An automatic proof of this identity has been described in Note 1.2.5.

Exercise 4.4.7. Let $A \in \mathbb{K}[x]$, $A \neq 0$, and $x_0 \in \mathbb{K}$ be a root of A. Prove the existence of a positive integer n such that

$$A(x) = (x - x_0)^n Q(x) \tag{4.4.6}$$

with $Q \in \mathbb{K}[x]$ and $Q(x_0) \neq 0$. The integer n is called the **multiplicity** of the root x_0. A **simple root** is one of multiplicity 1.

Exercise 4.4.8. Prove that a polynomial P has all simple roots if and only if it is relatively prime to its derivative P'. Conclude that it is possible to know if a polynomial has a repeated root without being able to find it.

Exercise 4.4.9. Let $\{x_i : 1 \leq i \leq r\}$ be the set of nonzero roots of $A(x)$ and let n_i be the multiplicity of x_i. Check that the polynomial A can be factored as

$$A(x) = Cx^{n_0} \prod_{i=1}^{r} \left(1 - \frac{x}{x_i}\right)^{n_i} \tag{4.4.7}$$

with $n_0 \geq 0$ is the multiplicity of $x = 0$ as a root of A.

Exercise 4.4.10. The value $z_0 \in \mathbb{C}$ is called a **complex root** of A if $A(z_0) = 0$. Prove that if $z_0 = u + iv$ is a complex root of the real polynomial A, then so is its complex conjugate $\bar{z_0} = u - iv$. Check also that their multiplicities agree and

$$A(x) = (x^2 - 2ux + u^2 + v^2)^n A_1(x) \tag{4.4.8}$$

where n is the multiplicity of $u + iv$ and $A_1(x)$ is a real polynomial.

In the construction of number systems described in Chapter 1 it would have been possible to include **algebraic numbers** as an intermediate step between $\mathbb{Q}$ and $\mathbb{C}$. Some of the properties of these numbers are described next.

Definition 4.4.11. A complex number α is called **algebraic** if there is a polynomial $A(x)$, with integer coefficients, such that $A(\alpha) = 0$. The set of algebraic numbers is denoted by $\mathbb{A}$.

Example 4.4.12. The golden ratio $\varphi = (1 + \sqrt{5})/2$ is an algebraic number. It satisfies the equation $x^2 - x - 1 = 0$.

Note 4.4.13. The fundamental theorem presented in Section 4.5 shows that a polynomial with complex coefficients has all of its roots in $\mathbb{C}$. Therefore it is reasonable to assume, from the beginning, that algebraic numbers are inside $\mathbb{C}$.

Definition 4.4.14. Given an algebraic number α, let B be the polynomial of minimal degree with integer coefficients such that $B(\alpha) = 0$. This polynomial is determined uniquely by the requirements that its leading coefficient should be positive and that its coefficients have no common factor. This is the **minimal polynomial** of α.

Exercise 4.4.15. Find the minimal polynomial of the golden ratio φ. **Hint:** Example 4.4.12.

Note 4.4.16. The concept of minimal polynomial can be used to show that $\mathbb{A}$ satisfies some closure properties: given $\alpha_1, \alpha_2 \in \mathbb{A}$, then $\alpha_1 + \alpha_2$ and $\alpha_1\alpha_2 \in \mathbb{A}$. It is actually difficult to prove that a specific number is not algebraic; such numbers are called **transcendental**. Two examples are discussed in later chapters. The fact that e is transcendental is presented in detail in the proof of Theorem 11.5.7. The same result holds for π; this is just stated as Theorem 12.13.8. A very nice introduction to transcendence questions is provided in the book by E. B. Burger and R. Tubbs [**86**]. On the other hand, from the point of view of cardinality, it is not hard to show that most complex numbers are transcendental numbers. The next theorem states this in more concrete form. The proof parallels that of Theorem 1.8.16.

Theorem 4.4.17. *The set of algebraic numbers is countable.*

Proof. Define the height of a polynomial with integer coefficients $A(x) = a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n$ by

$$h(A) = |n| + \sum_{j=0}^{n} |a_j|. \tag{4.4.9}$$

The height of an algebraic number is defined to be the height of its minimal polynomial. To complete the proof, use Exercise 1.8.15 and observe that there are finitely many polynomials of a given height. □

4.5. The fundamental theorem of algebra

The construction of number fields described in Chapter 1 proceeds by adjoining roots of polynomials to obtain $\mathbb{Z}$ from $\mathbb{N}$ and $\mathbb{Q}$ from $\mathbb{Z}$. The next step in the chain, namely from $\mathbb{Q}$ to $\mathbb{R}$, is analytic in nature, involving the idea of completion. The last step, from $\mathbb{R}$ to $\mathbb{C}$, is defined by adjoining a **single** root of the polynomial $A(x) = x^2+1$. It is a remarkable fact that the complex numbers are **complete** and **algebraically closed**: every polynomial with complex coefficients has all its roots in $\mathbb{C}$. This result is known as the **fundamental theorem of algebra**.

Theorem 4.5.1. *Every complex polynomial of degree $n > 0$ has a root in $\mathbb{C}$.*

The proof presented here is due to F. Terkelsen [**290**]. The first step is to show that nonconstant polynomials converge uniformly to ∞ as $|x| \to \infty$.

Lemma 4.5.2. *Let A be a complex polynomial of degree $n > 0$. Then there are positive constants c_1, c_2, R, depending only on the coefficients of A, such that*

$$c_1|x|^n \leq |A(x)| \leq c_2|x|^n \tag{4.5.1}$$

for $|x| \geq R$.

Proof. Let $A(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$. To establish an upper bound, define

$$R = \max\{1, |a_0|, |a_1|, \ldots, |a_n|\}. \tag{4.5.2}$$

Then, for $|x| > R$, the inequality $|x|^j \leq |x|^n$ gives

$$\begin{aligned} |A(x)| &\leq |a_n||x|^n + |a_{n-1}||x|^{n-1} + \cdots + |a_n| \\ &\leq |x|^n \left(|a_n| + |a_{n-1}| + \cdots + |a_0|\right) \\ &\leq (n+1)R|x|^n \end{aligned}$$

and the bound holds with $c_2 = (n+1)R$. The lower bound follows from $|A(x) - a_n x^n| \leq nR|x|^{n-1}$. The details are left to the reader. Observe that in the proof of the lower bound, the choice of R must involve the roots of A. □

Exercise 4.5.3. Provide all details in the previous proof.

Exercise 4.5.4. Let $n \in \mathbb{N}$ and $a \in \mathbb{C}$. Prove that the equation $x^n = a$ has n simple roots. For $a = 1$, the solutions to $x^n = 1$ are called **roots of unity**. **Hint:** Write the complex number in **polar form** and study the effect of powers on the radius and the angle. **Note:** This exercise is a special case of Theorem 4.5.1 and its result is actually used in the proof of the general case.

The proof of Theorem 4.5.1 is given next.

Proof. The continuity of $|A|$ shows that $|A|$ attains its minimum on every closed disk $\{x \in \mathbb{C} : |x| \leq r\}$. Lemma 4.5.2 shows the existence of a fixed $x_0 \in \mathbb{C}$ such that $|A(x_0)| \leq |A(x)|$ for all $x \in \mathbb{C}$. Replacing $A(x)$ by $A(x+x_0)$, it may be assumed that $x_0 = 0$. Suppose $A(0) \neq 0$ and write

$$A(x) = a + bx^m + x^{m+1}Q(x) \tag{4.5.3}$$

where $m \in \mathbb{N}$, $a = A(0) \neq 0$, $b \neq 0$, and Q is a complex polynomial. Now

$$A(tw) = a + bt^n w^m + (tw)^{m+1} Q(tw)$$

and Exercise 4.5.4 gives $w \in \mathbb{C}$ such that $w^m = -a/b$. Then

$$A(tw) = a(1 - t^m) + t^m \left(tw^{m+1} Q(tw) \right).$$

The continuity of Q permits us to choose $t \in (0, 1)$ small enough so that $|tw^{m+1} Q(tw)| < |a|$. Then

$$|A(tw)| < |a|(1 - t^m) + t^m |a| = |a| = |A(0)|.$$

This contradicts the minimality of $|A(0)|$. □

Corollary 4.5.5. *Let A be a complex polynomial of degree n. Then A has exactly n roots, counted according to multiplicity.*

The reader will find more information about the fundamental theorem of algebra and several other proofs in the book by B. Fine and G. Rosenberger [**127**].

4.6. The solution of polynomial equations

The problem of finding the roots of a polynomial equation

$$P_n(x) = a_0 x^n + a_1 x^{n-1} + \cdots + a_n \tag{4.6.1}$$

as a function of the coefficients $\{a_0, a_1, \ldots, a_n\}$ was one of the main driving forces behind the development of algebra for many centuries.

This section describes a solution to this problem for polynomials of low degree following a uniform procedure due to M. J. Hellman [**164, 165**]. This treats the polynomials of degree at most 4. Moreover, it also hints at the difficulties encountered when trying to solve quintic equations.

The presentation starts by describing the solution of a special important case.

Theorem 4.6.1. *Assume P_n has integer coefficients. Then the reduced form of any rational root of $P_n(x) = 0$ has the form $x = p/q$, where p is a divisor of a_n and q is a divisor of a_0.*

Proof. The identity $P_n(x) = 0$ implies

$$a_0p^n + a_1p^{n-1}q + \cdots + a_{n-1}pq^{n-1} + a_nq^n = 0. \tag{4.6.2}$$

This shows that q divides a_0p^n, so it must divide a_0. The same argument shows that p must divide a_n. □

Example 4.6.2. The polynomial $T(x) = 8x^3 - 4x^2 - 4x + 1$ will appear in Example 12.9.9. The previous theorem gives the irreducibility of T. Indeed, if T were reducible over $\mathbb{Q}$, then it would have a rational root. These roots are among the numbers $\{1, 2, 4, 8, -1, -2, -4, -8\}$ and it is easy to check that none of these values are roots of T.

The general analysis for polynomials of low degree is presented next.

Quadratic polynomials. These have the form

$$P_2(x) = a_0x^2 + a_1x + a_2 \tag{4.6.3}$$

and the equation $P_2(x) = 0$ may be solved by **completing the square** as every school-age child knows:

$$P_2(x) = a_0\left(\left(x + \frac{a_1}{2a_0}\right)^2 - \frac{D}{4a_0^2}\right), \tag{4.6.4}$$

where

$$D := a_1^2 - 4a_0a_2 \tag{4.6.5}$$

is the **discriminant** of the polynomial P_2. The **quadratic formula** has appeared.

Theorem 4.6.3. *The roots of* $P_2(x) = 0$ *are given by*

$$x_1 = \frac{-a_1 + \sqrt{D}}{2a_0} \quad \textit{and} \quad x_2 = \frac{-a_1 - \sqrt{D}}{2a_0}. \tag{4.6.6}$$

Note 4.6.4. Denote the roots of $P_2(x) = 0$ by x_1 and x_2. Then

$$a_0x^2 + a_1x + a_2 = a_0(x - x_1)(x - x_2)$$

yields

$$x_1 + x_2 = -a_1/a_0 \quad \text{and} \quad x_1x_2 = a_2/a_0.$$

This produces

$$(x_1 - x_2)^2 = (x_1 + x_2)^2 - 4x_1x_2 = \frac{a_1^2}{a_0^2} - \frac{4a_2}{a_0} = \frac{D}{a_0^2}.$$

Extracting the square root gives the expressions (4.6.6).

Note 4.6.5. The **symmetric functions** of the roots x_1, x_2 are

$$e_1 = x_1 + x_2 = -a_1/a_0 \quad \text{and} \quad e_2 = x_1x_2 = a_2/a_0. \tag{4.6.7}$$

These values admit an elementary geometric interpretation. The vertex of the parabola $y = P_2(x)$ is located at

$$(V_x, V_y) = \left(-\frac{a_1}{2a_0}, P_2\left(-\frac{a_1}{2a_0}\right)\right) = \left(-\frac{a_1}{2a_0}, -\frac{D}{4a_0}\right),$$

so that

$$V_x = \frac{x_1 + x_2}{2}. \tag{4.6.8}$$

Since V_x is the arithmetic mean of the zeros, it may be worthwhile to look at the (population) variance. A direct calculation shows that

$$\sigma^2 = \frac{D}{4a_0^2} = -\frac{V_y}{a_0}, \tag{4.6.9}$$

that is, $V_y = -a_0\sigma^2$.

Cubic polynomials. The next example considers the solution of the cubic polynomial

$$P_3(x) = a_0x^3 + a_1x^2 + a_2x + a_3. \tag{4.6.10}$$

The history of this quest, conducted mainly by G. Cardano, N. Fontana (nicknamed Tartaglia), and L. Ferrari is documented in the textbook by J. P. Tignol [**291**].

The reduction $y = x - a_1/3a_0$ eliminates the quadratic term and converts P_3 into the **reduced form**

$$P_3(y) = a_0y^3 + \frac{3a_0a_2 - a_1^2}{3a_0}y + \frac{a_1(2a_1^2 - 9a_2a_0) + 27a_0^2a_3}{27a_0^2}.$$

Therefore, the equation $P_3(x) = 0$ is equivalent to

$$P_3^*(x) := x^3 + ax + b = 0 \tag{4.6.11}$$

with

$$(4.6.12) \qquad a := \frac{3a_0a_2 - a_1^2}{3a_0^2}, \quad b := \frac{2a_1^3 - 9a_0a_1a_2 + 27a_0^2a_3}{27a_0^3}$$

going back to x as the independent variable.

Exercise 4.6.6. Compute the reduced form of $6x^3-13x^2+9x-2=0$.

Let x_1, x_2, x_3 be the roots of $P_3^*(x)=0$. Comparing the coefficients in

$$x^3+ax+b=(x-x_1)(x-x_2)(x-x_3)$$

yields

$$(4.6.13) \qquad \begin{aligned} x_1+x_2+x_3 &= 0, \\ x_1x_2+x_2x_3+x_3x_1 &= a, \\ x_1x_2x_3 &= -b. \end{aligned}$$

Adding the three equations, $P_3^*(x_i)=0$, and using (4.6.13) produces

$$(4.6.14) \qquad x_1^3+x_2^3+x_3^3-3x_1x_2x_3=0,$$

which factors as

$$(x_1+x_2+x_3)(x_1+\omega x_2+\omega^2x_3)(x_1+\omega^2x_2+\omega x_3)=0,$$

where $\omega^3=1$, $\omega \neq 1$. There are three possibilities:

$$x_1=-(x_2+x_3), \quad x_1=-(\omega x_2+\omega^2x_3), \quad \text{or} \quad x_1=-(\omega^2x_2+\omega x_3).$$

This form suggests the parametrization

$$(4.6.15) \quad x_1=-(s+t), \; x_2=-(\omega s+\omega^2t), \; \text{and } x_3=-(\omega^2s+\omega t),$$

where s and t will be chosen in order to satisfy (4.6.13). The first equation in (4.6.13) is automatically satisfied and the other two yield

$$(4.6.16) \qquad s^3t^3=-\frac{a^3}{27} \quad \text{and} \quad s^3+t^3=b.$$

To find the solutions, let $u=s^3$ and $v=t^3$ to produce a system in (u,v). Its solution yields

$$s=\left(\frac{b}{2}+\sqrt{\frac{b^2}{4}+\frac{a^3}{27}}\right)^{1/3} \quad \text{and} \quad t=\left(\frac{b}{2}-\sqrt{\frac{b^2}{4}+\frac{a^3}{27}}\right)^{1/3}.$$

These results are summarized in the next theorem. The expression for the roots involves the discriminant defined next.

Definition 4.6.7. The **discriminant** of the reduced cubic polynomial $P_3(x) = x^3 + ax + b$ is

$$D = \frac{4a^3 + 27b^2}{108}. \tag{4.6.17}$$

The next theorem gives the roots of a cubic equation.

Theorem 4.6.8. *The roots of the cubic equation* $P_3(x) = a_0x^3 + a_2x + a_1x + b$ *can be expressed by radicals in terms of the coefficients. To obtain the explicit parametrization, compute the reduced form* $P_3^*(x) = x^3 + ax + b$ *with*

$$a := \frac{3a_0a_2 - a_1^2}{3a_0^2}, \qquad b := \frac{2a_1^3 - 9a_0a_1a_2 + 27a_0^2a_3}{27a_0^3}.$$

Let D *be the discriminant of the cubic*

$$D = \frac{4a^3 + 27b^2}{108}, \tag{4.6.18}$$

and introduce the parameters

$$s = \left(\frac{b}{2} + \sqrt{D}\right)^{1/3}, \qquad t = \left(\frac{b}{2} - \sqrt{D}\right)^{1/3},$$

and $\omega = \frac{1}{2}(-1 + i\sqrt{3})$. *Then the roots of* $P_3^*(x) = 0$ *are given by*

$$x_1 = -(s + t), \quad x_2 = -(\omega s + \omega^2 t), \quad \text{and} \quad x_3 = -(\omega^2 s + \omega t).$$

Note 4.6.9. The expression for the roots of a cubic polynomial given in Theorem 4.6.8 was motivated by the goal of **solving the equation by radicals**. An alternative form of the solution can be obtained by expressing these roots in terms of a trigonometric function. This departure from the algebraic setting is simpler and it will be described in detail in Chapter 12. It is based on the idea of reducing the cubic to a normal form given by the identity

$$\sin 3u = -4\sin^3 u + 3\sin u. \tag{4.6.19}$$

It turns out that this alternative form of solving a cubic equation generalizes to polynomial equations of any degree. Note 5.2.8 has details. Naturally, the trigonometric functions are replaced by a different type of function.

Note 4.6.10. The development of complex numbers had as one of its sources the so-called **casus irreducibilis**. This refers to the situation of an irreducible cubic polynomial with integer coefficients and three distinct real roots. The procedure developed by Cardano to find these roots involves the computations of square roots of negative numbers. The reader should follow Cardano's procedure in the example

$$P(x) = x^3 - 6x^2 + 9x - 1. \tag{4.6.20}$$

A second cubic polynomial will appear naturally as Example 12.9.9.

4.7. Cubic polynomials

The cubic polynomial

$$y = P_3(x) = a_0x^3 + a_1x^2 + a_2x + a_3 \tag{4.7.1}$$

has either three simple real roots, a simple real root and a real root of multiplicity 2, a single real root and a pair of nonreal complex conjugate roots, or a single real root of multiplicity 3. This section develops a criterion for distinguishing these three situations. An application to a dynamical system is presented in Chapter 15.

The number of parameters in the equation $P_3(x) = 0$ is reduced by a **normalization** described next. It is assumed that a_3, $a_0 \neq 0$.

Reduction 1. The coefficient a_0 is 1.

Proof. The leading coefficient $a_0 \neq 0$. Dividing $P_3(x) = 0$ by a_0 yields the first reduction. □

Reduction 2. The coefficient a_3 is 1.

Proof. Introduce the scaling $x = \lambda t$ to transform $P_3(x) = 0$ into

$$t^3 + \frac{a_1}{\lambda}t + \frac{a_2}{\lambda^2}t + \frac{a_3}{\lambda^3} = 0.$$

The choice $\lambda = a_3^{1/3}$ gives the desired reduction. □

Definition 4.7.1. The **normalization** of $P_3(x) = 0$ is given by the cubic equation

$$P(x) = x^3 + ax^2 + bx + 1 = 0. \tag{4.7.2}$$

The nature of the roots of the normalized form of a cubic polynomial is described next. These roots are denoted by x_1, x_2, x_3. Then

$$x^3 + ax^2 + bx + 1 = (x - x_1)(x - x_2)(x - x_3). \tag{4.7.3}$$

Lemma 4.7.2. *The normalized polynomial has at least one negative real root.*

Proof. The values $P(0) = 1$ and $P(-\infty) = -\infty$ give the result. □

In the factorization (4.7.3), assume that $x_1 < 0$. The identity $x_1x_2x_3 = -1$ shows that there are three possible cases for the remaining roots.

Case 1. Three real roots $x_1 \leq x_2 \leq x_3 < 0$.

Case 2. Three real roots $x_1 < 0 < x_2 \leq x_3$.

Case 3. One real root $x_1 < 0$ and a pair $x_2 = u + iv$, $x_3 = u - iv$ of complex conjugate roots.

Lemma 4.7.3. *Assume $a^2 < 3b$. Then Case 3 occurs.*

Proof. The derivative $P'(x) = 3x^2 + 2ax + b$ is always positive because its discriminant is $4(a^2 - 3b) < 0$. Therefore P has a single real root. □

Lemma 4.7.4. *Assume $a^2 = 3b$ and $a \neq 3$. Then*

$$P(x) = (x + a/3)^3 + \tfrac{1}{27}(27 - a^3). \tag{4.7.4}$$

This corresponds to Case 3.

Proof. The derivative of P is

$$\begin{aligned} P'(x) &= 3x^2 + 2ax + b \\ &= 3\left((x + a/3)^2 + (3b - a^2)/9\right) \\ &= 3(x + a/3)^2. \end{aligned}$$

Integrate and use the condition $P(0) = 1$ to obtain the result. □

Lemma 4.7.5. *Assume $a^2 = 3b$ and $a = 3$. Then $P(x) = (x + 1)^3$. This corresponds to Case 1 with three equal roots $x_1 = x_2 = x_3 = -1$.*

Proof. Start as in the proof of Lemma 4.7.4 to obtain (4.7.4). The condition $a = 3$ shows that $P(x) = (x+1)^3$. □

The last case to consider is $a^2 > 3b$.

Lemma 4.7.6. *Assume $a^2 > 3b$. Then the derivative $P'(x) = 3x^2 + 2ax + b$ actually changes sign.*

Proof. Assume $P'(x) \geq 0$ for all $x \in \mathbb{R}$. The conditions on the parameters show that $P'(x)$ has real roots. Therefore P' must have a double root. The only root of $P''(x)$ is $x = -a/3$ and $P'(-a/3) = -(a^2 - 3b)/3 < 0$. This is a contradiction. □

The previous lemma shows that the polynomial has a minimum at

$$x_{\text{min}} = \frac{1}{3}(-a + \sqrt{a^2 - 3b}) \tag{4.7.5}$$

and a maximum at

$$x_{\text{max}} = \frac{1}{3}(-a - \sqrt{a^2 - 3b}). \tag{4.7.6}$$

The next step is to compute the values of P at these critical points.

Lemma 4.7.7. *The value at the minimum is given by*

$$P(x_{\text{min}}) = \frac{27 + 2a^3 - 9ab}{27} - \frac{2}{27}(a^2 - 3b)^{3/2}$$

and at the maximum, the polynomial attains the value

$$P(x_{\text{max}}) = \frac{27 + 2a^3 - 9ab}{27} + \frac{2}{27}(a^2 - 3b)^{3/2}.$$

The next step is to characterize roots of multiplicity 2.

Lemma 4.7.8. *The polynomial $P(x) = x^3 + ax^2 + bx + 1$ has a double root if and only if*

$$4a^3 + 4b^3 - a^2b^2 - 18ab + 27 = 0. \tag{4.7.7}$$

Proof. There are two possible case according to whether the double root occurs at the minimum or the maximum. In the first case, $P(x_{\min}) = 0$ yields

$$\frac{27 + 2a^3 - 9ab}{27} = \frac{2}{27}(a^2 - 3b)^{3/2}. \tag{4.7.8}$$

This requires first that $27 + 2a^3 - 9ab \geq 0$ and squaring both sides of (4.7.8) produces (4.7.7). In the second case, $P(x_{\max}) = 0$ gives

$$-\frac{27 + 2a^3 - 9ab}{27} = \frac{2}{27}(a^2 - 3b)^{3/2} \tag{4.7.9}$$

and now $27 + 2a^3 - 9ab \leq 0$ and squaring yields (4.7.7), again. □

Definition 4.7.9. The function

$$R(a, b) = 4a^3 + 4b^3 - a^2b^2 - 18ab + 27 \tag{4.7.10}$$

is called the **resolvent** of the polynomial $P_3(x) = x^3 + ax^2 + bx + 1$.

The next exercise shows the relation between the resolvent defined above and the discriminant of the cubic polynomial.

Exercise 4.7.10. Let $P(x) = x^3 + ax^2 + bx + 1$. Check that the resolvent $R(a, b)$ is the discriminant of the reduced form of P, given by

$$P_*(x) = x^3 + (b - a^2/3)x + (1 + 2a^3/27 - ab/3), \tag{4.7.11}$$

obtained from P by eliminating the quadratic term.

Exercise 4.7.11. Assume $b \neq 0$ and $a^2 > 3b$. Establish the following criteria:

Case 1 occurs if and only if $x_{\min} < 0$ and $P(x_{\min}) < 0$.

Case 2 occurs if and only if $x_{\min} > 0$ and $P(x_{\min}) < 0$.

Case 3 occurs if and only if $P(x_{\min}) > 0$.

Develop also a similar result for the case $b = 0$.

The final description of the type of roots for a cubic polynomial is given in the next theorem.

Theorem 4.7.12. *Let*

$$R(a, b) = 4a^3 + 4b^3 - a^2b^2 - 18ab + 27$$

be the discriminant of the cubic polynomial $P_3(x) = x^3 + ax^2 + bx + 1$. *Then the cubic equation has*

- *one real root and a complex conjugate pair if and only if* $R > 0$,
- *two distinct real roots if and only if* $R = 0$ *and* $a^2 \neq 3b$,
- *three distinct real roots if and only if* $R < 0$,
- *three equal roots if and only if* $R = 0$ *and* $a^2 = 3b$.

The graph of the resolvent curve $R(a, b) = 0$ is shown in Figure 4.7.1. This curve will reappear in Chapter 15.

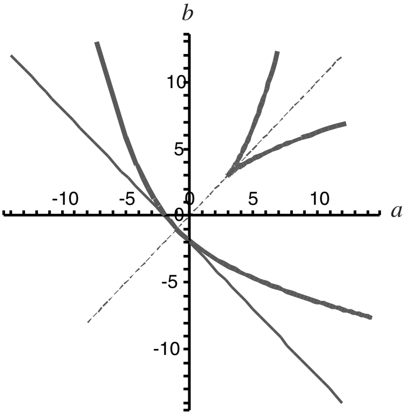


Figure 4.7.1. The resolvent curve.

Exercise 4.7.13. Provide a detailed proof of Theorem 4.7.12.

4.8. Quartic polynomials

This section considers the solution of the quartic equation

$$P_4(x) = a_0x^4 + a_1x^3 + a_2x^2 + a_3x + a_4 = 0. \tag{4.8.1}$$

The first step is a reduction of the form of P_4.

Exercise 4.8.1. Prove that the quartic equation may be reduced to the form

$$x^4 + ax^2 + bx + c = 0.$$

Theorem 4.8.2. *The roots of* $P_4(x) = 0$ *can be reduced to the solution of a cubic equation.*

Proof. Start with the reduced form $x^4 + ax^2 + bx + c = 0$ and let x_1, x_2, x_3, x_4 be its roots. Then

$$x^4 + ax^2 + bx + c = (x - x_1)(x - x_2)(x - x_3)(x - x_4)$$

produces

$$\begin{aligned} x_1 + x_2 + x_3 + x_4 &= 0, \\ x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4 &= a, \\ x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + x_2x_3x_4 &= -b, \\ x_1x_2x_3x_4 &= c. \end{aligned} \tag{4.8.2}$$

Introduce new parameters by

$$u = x_1 + x_2, \quad v = x_3 + x_4, \quad s = x_1x_2, \quad t = x_3x_4 \tag{4.8.3}$$

to transform (4.8.2) to

$$u + v = 0, \quad s + t + uv = a, \quad sv + tu = -b, \quad st = c.$$

This reduces to

$$\begin{aligned} s + t &= a + u^2, \\ u(s - t) &= b, \\ st &= c. \end{aligned} \tag{4.8.4}$$

Solve for s and t to obtain

$$s = \frac{1}{2}\left(a + u^2 + \frac{b}{u}\right), \qquad t = \frac{1}{2}\left(a + u^2 - \frac{b}{u}\right). \tag{4.8.5}$$

Replacing in the last equation of (4.8.4) yields

$$u^6 + 2au^4 + (a^2 - 4c)u^2 - b^2 = 0. \tag{4.8.6}$$

This is a *cubic* equation in u^2. The solution is replaced in (4.8.5) to obtain the value of s. The roots x_1 and x_2 can now be obtained from (4.8.3). Finally, employ the relations $v = -u$ and $t = c/s$ to produce the values of x_3 and x_4. □

Exercise 4.8.3. Use this procedure to solve the quartic equation

$$42x^4 - 281x^3 + 372x^2 - 81x - 20 = 0.$$

Exercise 4.8.4. The previous approach fails to produce a solution to the quintic equation

$$P_5(x) = a_0x^5 + a_1x^4 + a_2x^3 + a_3x^2 + a_4x + a_5 = 0. \tag{4.8.7}$$

Check the details. Start by normalizing P_5 by assuming $a_0 = 1$ and $a_2 = 0$. Let $\{x_1, x_2, x_3, x_4, x_5\}$ be the roots of P_5. Introduce the notation

$$s = x_1 + x_2 + x_3, \qquad t = x_1x_2 + x_1x_3 + x_2x_3,$$
$$v = x_1x_2x_3, \qquad w = x_4x_5.$$

Observe that $x_4 + x_5 = s$. Establish the relations

$$-s^2 + t + w = a_2, \qquad -st + sw + v = -a_3,$$
$$tw - sv = a_4, \qquad vw = -a_5.$$

Solve for t and v to produce the relation

$$\begin{aligned} -s^2w^2 + a_4w - a_5s + w^3 &= a_2w^2, \\ a_5s^2 - a_4sw + sw^3 - a_5w &= -a_3w^2. \end{aligned}$$

Eliminating s or w gives an equation of degree higher than 5.

Note 4.8.5. One of the achievements of mathematics in the nineteenth century was to show that it is impossible to express the roots x_i of the general equation (4.8.7) **by radicals**. That is, there is no finite combination of radicals of the coefficients a_i that gives the roots. Naturally it is possible that there are other analytic expressions in the coefficients $\{a_i\}$ that give the roots. The reader will find information about this problem in the book [**213**] and in the text by J. Shurman [**273**]. The subject is full of beautiful interconnections. Who would suspect that the solution of a quintic polynomial would be related to the **icosahedron**, one of the **platonic solids** of antiquity?

Chapter 5

Binomial Sums

5.1. Introduction

This chapter deals with the question of explicit evaluations of finite sums involving binomial coefficients. The discussion is restricted to sums of the type

$$M_{i,j}(n) = \sum_{k=0}^{n} k^i \binom{n}{k}^j \tag{5.1.1}$$

including the special case

$$L_j(n) = \sum_{k=0}^{n} \binom{n}{k}^j . \tag{5.1.2}$$

The proofs are based on recurrences, some combinatorial arguments, and an introduction to automatic methods.

These examples are part of the class of **hypergeometric sums**:

$$f(n) = \sum_{k=0}^{n} F(n,k) \tag{5.1.3}$$

where $F(n,k)$ is a hypergeometric function in both variables, that is, the ratios

$$\frac{F(n+1,k)}{F(n,k)} \quad \text{and} \quad \frac{F(n,k+1)}{F(n,k)} \tag{5.1.4}$$

are rational functions of n and k. These sums have a long history and recently they have been placed in a general framework by the work of H. Wilf and D. Zeilberger and described in the book [**247**] written jointly with M. Petkovsek. An introduction to these ideas is given below.

The examples include the classical evaluations

$$L_1(n) = \sum_{k=0}^{n} \binom{n}{k} = 2^n \quad \text{and} \quad L_2(n) = \sum_{k=0}^{n} \binom{n}{k}^2 = \binom{2n}{n}$$

as well as a discussion of the fact that

$$L_3(n) = \sum_{k=0}^{n} \binom{n}{k}^3 \tag{5.1.5}$$

does not have a similar closed-form evaluation. The author has always been intrigued by this phenomenon.

5.2. Power sums

The sum

$$L_j(n) = \sum_{k=0}^{n} \binom{n}{k}^j, \qquad \text{for } j \in \mathbb{N}, \tag{5.2.1}$$

named here **power sums**, are considered next.

5.2.1. The first power. The case $j = 1$ deals with the elementary identity

$$L_1(n) = \sum_{k=0}^{n} \binom{n}{k} = 2^n. \tag{5.2.2}$$

Several proofs are presented.

Proof 1. The binomial theorem

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}, \tag{5.2.3}$$

with $a = b = 1$, gives the result.

Proof 2. The argument is of a combinatorial nature. Corollary 2.2.3 states that the number of subsets of $[n] := \{1, 2, \ldots, n\}$ with k elements is given by $\binom{n}{k}$. The total number of subsets is 2^n. The left-hand side of the identity (5.2.2) corresponds to counting subsets of $[n]$ conditioned on the number of elements.

Proof 3. The next proof is based on recurrences. The main idea is to first produce a recurrence for the summand $\binom{n}{k}$ and then to sum over all the values of k to obtain one recurrence for the sum. The next subsection indicates how to find the recurrence by an automatic procedure.

The binomial coefficients satisfy

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1} \tag{5.2.4}$$

as shown in Theorem 2.1.6. Now sum this recurrence over k. Observe that the vanishing of the binomial coefficient $\binom{n}{k}$ for $k < 0$ and $k > n$ shows that the sum over all $k \in \mathbb{Z}$ reduces to a finite sum. Indeed, the result is

$$\sum_{k=0}^{n} \binom{n}{k} = \sum_{k=0}^{n-1} \binom{n-1}{k} + \sum_{k=1}^{n} \binom{n-1}{k-1}, \tag{5.2.5}$$

which produces a recurrence for L_1 in the form

$$L_1(n) = 2L_1(n-1). \tag{5.2.6}$$

To verify (5.2.2), it suffices to check that 2^n satisfies the same recurrence and the same initial condition $L_1(1) = 2$. This is easy.

5.2.2. An automatic derivation of recurrences. The method of Sister Celine.

Sister Mary Celine Fasenmyer proposed a method to derive recurrences such as (5.2.4). The method has been superceded by more efficient algorithms, but its simplicity makes it an ideal introduction to the subject of **automatic proofs**.

Define

$$F(n,k) = \binom{n}{k} = \frac{n!}{k!(n-k)!} \tag{5.2.7}$$

and look for a relation of the form

$$a(n)F(n,k)+b(n)F(n+1,k)+c(n)F(n,k+1)+d(n)F(n+1,k+1) = 0$$

where the unknowns a, b, c, d are functions independent of k. To find these functions, divide the relation above by $F(n,k)$ to produce

$$a(n)+b(n)\frac{F(n+1,k)}{F(n,k)}+c(n)\frac{F(n,k+1)}{F(n,k)}+d(n)\frac{F(n+1,k+1)}{F(n,k)}=0.$$

The crucial point of the method is to observe that the quotients appearing above are rational functions of n and k. For example,

$$\frac{F(n+1,k)}{F(n,k)}=\frac{n+1}{n-k+1}. \tag{5.2.8}$$

It follows that

$$a(n)+\frac{n+1}{n-k+1}b(n)+\frac{n-k}{k+1}c(n)+\frac{n+1}{k+1}d(n)=0. \tag{5.2.9}$$

Clearing denominators produces

$$\begin{aligned}&[c(n)-a(n)]\,k^2+[na(n)+(n+1)b(n)-(2n+1)c(n)-(n+1)d(n)]k\\ &\quad+\big[(n+1)a(n)+(n+1)b(n)+n(n+1)c(n)+(n+1)^2d(n)\big]=0.\end{aligned}$$

The vanishing of each of the coefficients in the variable k leads to the system of equations

$$\begin{pmatrix}-1 & 0 & 1 & 0\\ n & n+1 & -(2n+1) & -(n+1)\\ 1 & 1 & n & n+1\end{pmatrix}\begin{pmatrix}a(n)\\ b(n)\\ c(n)\\ d(n)\end{pmatrix}=\begin{pmatrix}0\\0\\0\end{pmatrix}.$$

The solution is given by

$$a(n)=-d(n),\quad b(n)=0,\quad c(n)=-d(n) \tag{5.2.10}$$

with $d(n)$ arbitrary. Choosing $d(n)=1$ gives

$$-F(n,k)-F(n,k+1)+F(n+1,k+1)=0, \tag{5.2.11}$$

that is,

$$\binom{n+1}{k+1}=\binom{n}{k}+\binom{n}{k+1}. \tag{5.2.12}$$

This becomes (5.2.4) after replacing $\{n,k\}$ by $\{n-1,k-1\}$.

Note 5.2.1. Summing over all values of k gives, as before, the recurrence (5.2.6) for the sum $L_1(n)$.

Note 5.2.2. The `Mathematica` code described next, written by C. Koutschan, provides a basic implementation of Sister Celine's algorithm and produces the above recurrences in an automatic manner.

```
SisterCeline1[f_Function, F_[n_, k_], dn_Integer, dk_Integer] :=
    Module[{i, j, anz, sys, sol, pp, dp, Sn, Sk},
    anz = Flatten[Table[f[n + j, k + i], i, 0, dk, j, 0, dn]];
    anz = FunctionExpand[anz/f[n, k]];
    anz = Together[(PolynomialLCM @@ Denominator[anz])*anz];
    sys = PadRight[CoefficientList[#, k] & /@ anz];
    sol = Together[NullSpace[Transpose[sys]]];
    anz = Flatten[Table[Sn^j*Sk^i, i, 0, dk, j, 0, dn]];
    sol = PolynomialRemainder[#.anz, Sk - 1, Sk] & /@ sol;
    sol = Thread[Expand[sol*F[n, k]] == 0];
    Return[sol /.  Sn^j_.*F[n, k] -> F[n + j, k]];
];
```

The command

```
SisterCeline1[Function[{n,k},Binomial[n,k]],L1[n,k],1,1]
```

is asking for a relation of the form

$$a(n)F(n,k)+b(n)F(n+1,k)+c(n)F(n,k+1)+d(n)F(n+1,k+1)=0$$

for $F(n,k)=\binom{n}{k}$, as explained above. The parameters `dn` and `dk` indicate the order of the requested recurrence in the variables n and k, respectively. The values `dn` $=$ `dk` $=1$ state that a first-order recurrence in both variables is being sought. The output is the implied recurrence for the sum

$$L1[n,k]=\sum_k F(n,k). \tag{5.2.13}$$

This is given as

(5.2.14) `{-2L1[n,k] + L1[1+n,k] == 0},`

stating that the sum

$$L_1(n)=\sum_{k=0}^{n}\binom{n}{k} \tag{5.2.15}$$

satisfies

$$-2L_1(n) + L_1(n+1) = 0. \tag{5.2.16}$$

This is equivalent to (5.2.6).

5.2.3. The second power. The second sum

$$L_2(n) = \sum_{k=0}^{n} \binom{n}{k}^2 \tag{5.2.17}$$

appeared in the proof of Proposition 2.5.16 in the computation of the remainder of the central binomial coefficients modulo a prime. This sum has the value

$$L_2(n) = \sum_{k=0}^{n} \binom{n}{k}^2 = \binom{2n}{n}, \tag{5.2.18}$$

and several proofs are presented below.

Proof 1. The right-hand side is the coefficient of x^n in the expansion of $(1+x)^{2n}$. The computation of this coefficient from $(1+x)^n \times (1+x)^n$ yields

$$\binom{2n}{n} = \sum_{k=0}^{n} \binom{n}{k} \binom{n}{n-k}. \tag{5.2.19}$$

The symmetry of the binomial coefficients gives the result.

Proof 2. The sum $L_2(n)$ is a special case of the next result, known as the **Vandermonde identity**.

Theorem 5.2.3. *Let n, $m \in \mathbb{N}$. Then for $0 \leq r \leq n+m$*

$$\sum_{k=0}^{r} \binom{n}{k} \binom{m}{r-k} = \binom{n+m}{r}. \tag{5.2.20}$$

Proof. The first proof is analytic. Simply compare the coefficient of x^r in the identity $(1+x)^{n+m} = (1+x)^n \times (1+x)^m$. □

Combinatorial proof. Choose r objects from a set of n red balls and m blue balls. Ignoring the color produces the right-hand side of (5.2.20). Now take the color into consideration and suppose you choose k red balls (with $0 \leq k \leq r$). Then $r-k$ blue balls are chosen. Each index k represents a different configuration. The addition principle now gives the left-hand side of (5.2.20). Taking $r=n=m$ in Theorem 5.2.3 gives (5.2.18).

Proof 3. The third proof is based on a recurrence satisfied by the squares of the binomial coefficients. It is an elementary application of Sister Celine's method. The computations by hand become long and tedious. The point of the next exercise is that problems of this type should be done by using a symbolic package.

Exercise 5.2.4. Define $F(n,k) = \binom{n}{k}^2$. Prove that Sister Celine's method shows that there is no recurrence of the form

$$a_{0,0}F(n,k)+a_{1,0}F(n+1,k)+a_{0,1}F(n,k+1)+a_{1,1}F(n+1,k+1) = 0,$$

where $a_{i,j} = a_{i,j}(n)$. The change in notation for the unknowns is motivated in order to keep track of the shifts; that is, $a_{i,j}$ is the coefficient of $F(n+i,k+j)$.

Now look for a recurrence of order 2, that is, a relation of the form

$$\sum_{i=0}^{2}\sum_{j=0}^{2} a_{i,j}(n)F(n+i,k+j) = 0 \tag{5.2.21}$$

to prove that $\binom{n}{k}^2$ satisfies the recurrence

$$\begin{aligned} n\binom{n}{k}^2 - (2n-1)\left\{\binom{n-1}{k}^2 + \binom{n-1}{k-1}^2\right\} \\ +(n-1)\left\{\binom{n-2}{k}^2 - 2\binom{n-2}{k-1}^2 + \binom{n-2}{k-2}^2\right\} = 0. \end{aligned} \tag{5.2.22}$$

The last step in the derivation of a recurrence is to sum over all values of k. This yields

$$L_2(n) = \frac{2(2n-1)}{n}L_2(n-1). \tag{5.2.23}$$

The next exercise shows how to verify the closed form $L_2(n) = \binom{2n}{n}$.

Exercise 5.2.5. Define $X_2(n)$ by the relation $L_2(n) = \binom{2n}{n} X_2(n)$. Check that (5.2.23) becomes $X_2(n) = X_2(n-1)$. The value $X_2(1) = 1$ completes the proof of (5.2.18).

Note 5.2.6. The reader will find still one more proof of the identity $L_2(n) = \binom{2n}{n}$ in the paper by S. Minsker [**219**]. This one uses basic complex analysis.

Note 5.2.7. The code described in Note 5.2.2 now provides the recurrence in automatic form. The command

(5.2.24) $\texttt{SC[Function[\{n,k\},Binomial[n,k]}^2\texttt{],L2[n,k],1,1]}$

gives

$$\{\ \}, \tag{5.2.25}$$

indicating that there is no recurrence of first order satisfed by the summands in $L_2(n)$. The command

(5.2.26) $\texttt{SC[Function[\{n, k\},Binomial[n,k]}^2\texttt{],L2[n,k],2,2]}$

produces a recurrence for $\binom{n}{k}^2$ that leads to

$$L_2(n+2) = \frac{2(2n+3)}{n+2} L_2(n+1), \tag{5.2.27}$$

which is equivalent to (5.2.23).

Note 5.2.8. In the case of the sum

$$L_3(n) = \sum_{k=0}^{n} \binom{n}{k}^3,$$

the code above provides the recurrence

$$\begin{aligned}(n+3)^2(3n+4)&L_3(n+3)\\ &= 2(9n^3+57n^2+116n+74)L_3(n+2)\\ &\quad + (45n^3+240n^2+419n+240)L_3(n+1)\\ &\quad + 8(3n^3+13n^2+17n+7)L_3(n).\end{aligned}$$

The methods developed in $A = B$ (see [**247**]) show, in automatic manner, that this recurrence **has no solution** in the class of hypergeometric terms.

This result about $L_3(n)$ is similar, in flavor, to the question of solving algebraic equations. The basic question is to find a formula for the roots of a polynomial equation in terms of the coefficients. Adding the **extra condition** that the formula must be formed by a finite number of radicals produces a negative answer for degree 5 or higher. On the other hand, if one is willing to accept other types of formulas, then there is one for any degree. This result, due to H. Umemura, appears as an appendix to the book by D. Mumford [**228**]. The same question may be asked about the sums $L_j(n)$. Is there a class of functions, larger than hypergeometric, that will provide closed-form expressions for these sums?

Exercise 5.2.9. Explore divisibility properties of $L_3(n)$. In particular prove that $L_3(n)$ is always even and $\nu_2(L_3(n)) = 1$ if and only if n is a power of 2. This is similar to Theorem 2.7.6 for the sum $L_2(n) = \binom{2n}{n}$. Is the result valid for $L_j(n)$ for all $j \in \mathbb{N}$?

Exercise 5.2.10. Check that the sum $L_3(n)$ is never divisible by the primes in the list $\mathbb{L} := \{3, 11, 17, 19, 43\}$. Find the next prime in the list. Is it possible to characterize these prime numbers?

5.3. Moment sums

The second type of sums discussed here is

$$M_{i,j}(n) = \sum_{k=0}^{n} k^i \binom{n}{k}^j. \tag{5.3.1}$$

The special case $M_{0,j}(n)$ corresponds to the power sum $L_j(n)$ discussed in the previous section.

5.3.1. Moments of the first power sum.

The first example is

$$M_{i,1}(n) = \sum_{k=0}^{n} k^i \binom{n}{k}. \tag{5.3.2}$$

The binomial theorem is now employed to produce a recurrence for these sums. The case $i = 1$ is analyzed first.

Apply the Euler operator $\vartheta = x\frac{d}{dx}$, defined in (4.2.20), to the expansion of $(1+x)^n$ to obtain

$$\vartheta(1+x)^n = \sum_{k=0}^{n} k\binom{n}{k}x^k. \tag{5.3.3}$$

Then

$$M_{1,1}(n) = \vartheta(1+x)^n \quad \text{evaluated at } x = 1, \tag{5.3.4}$$

from which it follows that

$$\sum_{k=1}^{n} k\binom{n}{k} = n2^{n-1}. \tag{5.3.5}$$

Exercise 5.3.1. Give a combinatorial proof of this identity. **Hint:** In a group of n students choose one committee in all possible ways and in each such committee pick a president. The left-hand side comes from choosing the committee first; the right-hand side comes from choosing the president first.

A recurrence for the sums $M_{i,1}$ is presented next.

Theorem 5.3.2. *The sum $M_{i,1}(n)$ has the form*

$$M_{i,1}(n) = n2^{n-i}R_i(1,n)$$

where $R_i(x,n)$ is a polynomial satifying the recurrence

$$R_i(x,n) = [(n-i)x+1]\,R_{i-1}(x,n) + x(1+x)\frac{d}{dx}R_{i-1}(x,n)$$

and initial condition $R_1(x,n) = 1$.

Proof. Applying the operator ϑ yields

$$M_{i,1}(n) = \vartheta^i(1+x)^n \quad \text{evaluated at } x = 1. \tag{5.3.6}$$

Start with

$$\vartheta(1+x)^n = nx(1+x)^{n-1} \tag{5.3.7}$$

and define $R_i(x,n)$ by the identity

$$\vartheta^i(1+x)^n = nx(1+x)^{n-i}R_i(x,n). \tag{5.3.8}$$

An easy induction argument shows that $R_i(x,n)$ is a polynomial. The recurrence for R_i also comes from this argument. Observe that

$$\vartheta^{i+1}(1+x)^n = \vartheta\left(nx(1+x)^{n-i}R_i(x,n)\right)$$

and use the definition of R to obtain the result. □

Note 5.3.3. The first few values of $R_i(1,n)$ are given by

$$\begin{aligned} R_1(1,n) &= 1, \\ R_2(1,n) &= n+1, \\ R_3(1,n) &= n(n+3), \\ R_4(1,n) &= (n+1)(n^2+5n-2), \\ R_5(1,n) &= n(n^3+10n^2+15n-10). \end{aligned}$$

Exercise 5.3.4. Prove that $R_i(1,n)$ is divisible by n for i odd and by $n+1$ if i is even. Find other properties of $R_i(x,n)$.

5.3.2. Moments of the second power sum.

The sums

$$M_{i,2}(n) = \sum_{k=0}^{n} k^i \binom{n}{k}^2 \tag{5.3.9}$$

are considered next. The first result employs (5.2.22) to produce a recurrence for a polynomial associated to $M_{i,2}(n)$.

Theorem 5.3.5. *The polynomial*

$$Y_n(x) := \sum_{k=0}^{n} \binom{n}{k}^2 x^k \tag{5.3.10}$$

satisfies

$$Y_{n+1}(x) = \frac{2n+1}{n+1}(1+x)Y_n(x) - \frac{n}{n+1}(1-x)^2 Y_{n-1}(x). \tag{5.3.11}$$

The initial conditions are $Y_0(x) = 1$, $Y_1(x) = 1+x$.

Proof. This follows directly by multiplying (5.2.22) by x^k and summing over all values of k. The reduction employs reductions of the form

$$\sum_k \binom{n-1}{k-1}^2 x^k = x\sum_k \binom{n-1}{k-1}^2 x^{k-1} = x\sum_k \binom{n-1}{k}^2 x^k.$$

□

Note 5.3.6. The recurrence (5.3.11) will be employed to write Y_n in the form

$$Y_n(x) = (1-x)^n P_n\left(\frac{1+x}{1-x}\right), \tag{5.3.12}$$

where P_n is the **Legendre polynomial** described in Theorem 14.2.16.

Note 5.3.7. The sum $M_{i,2}(n)$ is given in terms of the Euler operator ϑ as

$$M_{i,2}(n) = \vartheta^i \, Y_n(x) \quad \text{evaluated at } x = 1. \tag{5.3.13}$$

Note 5.3.8. For fixed $i \in \mathbb{N}$, `Mathematica` is able to evaluate these sums symbolically. The resulting expressions grow in size and the author has been unable to predict the hidden pattern. For example,

$$M_{10,2}(n) = \frac{n^3 2^{2n-10}}{\sqrt{\pi}\, n!}\left(\frac{2n-11}{2}\right)! \times Z(n)$$

where

$$\begin{aligned} Z(n) = n^{12} + 10n^{11} - 55n^{10} - 430n^9 + 1419n^8 + 4410n^7 - 13545n^6 \\ - 5910n^5 + 28380n^4 - 12592n^3 - 2256n^2 + 2752n - 504. \end{aligned}$$

Some symbolic calculations with the sum $M_{i,2}(n)$ suggest the following pattern: define

$$q_j(n) = \begin{cases} n^2 & \text{if } j \text{ is even,} \\ \frac{1}{2}n^3 & \text{if } j \text{ is odd} \end{cases}$$

and

$$W_j(n) := \frac{(n-1)!\,(n-\lfloor \frac{j}{2} \rfloor)!}{(2n-2\lfloor \frac{j}{2} \rfloor)!\, q_j(n)} \sum_{k=0}^{n} k^j \binom{n}{k}^2.$$

Then

$$W_1(n) = \frac{1}{n^3}, \quad W_2(n) = 1, \quad W_3(n) = \frac{n+1}{n},$$

and for $j \geq 4$, the expression $W_j(n)$ is a polynomial in n of degree $3\lfloor \frac{j-2}{2} \rfloor$. The first few examples are

$$\begin{aligned} W_4(n) &= n^3 + n^2 - 3n - 1, \\ W_5(n) &= (n+1)(n^2 + 2n - 5), \\ W_6(n) &= n^6 + 3n^5 - 13n^4 - 15n^3 + 30n^2 + 8n - 2, \\ W_7(n) &= (n+1)(n^5 + 5n^4 - 15n^3 - 35n^2 + 70n - 14). \end{aligned}$$

Exercise 5.3.9. Find a recurrence for the function $W_j(n)$ and prove that $W_j(n)$ is a polynomial. Discover and establish some of its properties.

5.4. Recurrences for powers of binomials

The recurrences for the sums

$$L_j(n) = \sum_{k=0}^{n} \binom{n}{k}^j \tag{5.4.1}$$

for $j = 1$ and $j = 2$ are elementary. In this section the case $j \geq 3$ is described. These sums appeared in two papers by J. Franel [**130, 131**]. The interest for these sums was revived when A. van der Poorten [**296**] described the proof by R. Apéry [**25**] that

$$\zeta(3) := \sum_{n=1}^{\infty} \frac{1}{n^3} \tag{5.4.2}$$

is an irrational number. Apéry's proof is based on the fact that

$$u_n = \sum_{k=0}^{n} \binom{n}{k}^2 \binom{n+k}{k}^2 \tag{5.4.3}$$

satisfies the recurrence

$$n^3 u_n - (34n^3 - 51n^2 + 27n - 5)u_{n-1} + (n-1)^3 u_{n-2} = 0. \tag{5.4.4}$$

The irrationality of $\zeta(3)$ is discussed in detail in Section 16.10.

Exercise 5.4.1. Find a hypergeometric representation of the number u_n in (5.4.3).

J. Franel showed in [**130**] that $L_3(n)$ satisfies the recurrence

$$(n+1)^2 L_3(n+1) - (7n^2 + 7n + 2)L_3(n) - 8n^2 L_3(n-1) = 0$$

and, in [**131**], that $L_4(n)$ satisfies

$$\begin{aligned}(n+1)^3 L_4(n+1) - 2(6n^3 + 9n^2 + 5n + 1)L_4(n) \\ - (4n+1)(4n)(4n-1)L_4(n-1) = 0.\end{aligned} \tag{5.4.5}$$

The search for recurrences was continued by M. A. Perlstadt in [**246**] who showed that $L_5(n)$ satisfies

$$b_0(n)L_5(n+1) + b_1(n)L_5(n) + b_2(n)L_5(n-1) + b_3(n)L_5(n-2) = 0,$$

with

$$\begin{aligned}
b_0(n) &= (n+1)^4(55n^2-77n+28),\\
b_1(n) &= -1155n^6-693n^5+732n^4+715n^3-45n^2-210n-56,\\
b_2(n) &= -19415n^6+27181n^5-7453n^4-3289n^3+956n^2+276n-96,\\
b_3(n) &= 32(n-1)^4(55n^2+33n+6).
\end{aligned}$$

A similar recurrence for $L_6(n)$ was described in [**246**] and an explanation for this type of recurrences was provided in the paper by T. W. Cusick [**107**]. The theory developed in [**247**] proves the existence of these recurrences. The `Mathematica` package `HolonomicFunctions`, written by C. Koutschan and accessible from his website, gives these recurrences in automatic form: the commands

```
ctS[j_] := CreativeTelescoping[Binomial[n,k]∧j,S[k]-1,{S[n]}],
opS[j_] := ctS[j][[1,1]]
```

are used to obtain these recurrences. For instance, the input

```
opS[1]
```

yields the output

$$S_n - 2 \tag{5.4.6}$$

with S_n being the shift operator in the variable n. The output must be interpreted as follows: the sum

$$L_1(n) := \sum_{k=0}^{n} \binom{n}{k} \tag{5.4.7}$$

satisfies the recurrence

$$L_1(n+1) - 2L_1(n) = 0. \tag{5.4.8}$$

This is (5.2.16). The main contribution of the papers by T. W. Cusick [**107**], M. A. Perlstadt [**246**], J. Yuan, Z. Lu, and A. L. Schmidt [**316**], and others can now be obtained via this package. For example,

```
opS[4]
```

yields the Franel recurrence (5.4.5) as

$$(2+n)^3S_n^2 - 2(3+2n)(7+9n+3n^2)S_n - 4(1+n)(3+4n)(5+4n).$$

Exercise 5.4.2. Experiment with the package `HolonomicFunctions`.

5.5. Calkin's identity

The literature contains many other finite sums involving binomial coefficients. The question of closed-form evaluations is rather difficult. This section considers the example

$$A_{n,i} = \sum_{k=0}^{i} \binom{n}{k}, \quad \text{for } 0 \leq i \leq n, \tag{5.5.1}$$

for which there seems to be no elementary expression aside from $A_{n,0} = 1$ and $A_{n,n} = 2^n$. This is sometimes called an **incomplete binomial sum**. The limits of summation are not natural, in the sense that the summand does not vanish outside the range of summation. `Mathematica` gives the evaluation

$$A_{n,i} = 2^n - \binom{n}{i+1} {}_2F_1\left[1,\, 1+i-n;\, i+2; -1\right]. \tag{5.5.2}$$

The **hypergeometric function** ${}_2F_1$ appearing in the answer is defined by the power series

$${}_2F_1(a, b; c; x) = \sum_{k=0}^{\infty} \frac{(a)_k\,(b)_k}{(c)_k\,k!} x^k, \tag{5.5.3}$$

where $(a)_k$ is the **Pochhammer symbol**, already defined in (2.1.9) by

$$(a)_k = \begin{cases} a(a+1)(a+2)\cdots(a+k-1) & \text{for } k > 0, \\ 1 & \text{if } k = 0. \end{cases} \tag{5.5.4}$$

Exercise 5.5.1. Prove that the series ${}_2F_1$ reduces to a finite sum if a or b is a negative integer. Confirm the identity (5.5.2).

Exercise 5.5.2. Check that ${}_2F_1(a, b; c; x)$ satisfies the differential equation

$$x(1-x)\frac{d^2y}{dx^2} + \left[c - (a+b+1)x\right]\frac{dy}{dx} - ab\,y(x) = 0.$$

Note 5.5.3. Two variants of the sum $A_{n,i}$ that do have closed-form expressions are the alternating version

$$\sum_{k=0}^{i} (-1)^k \binom{n}{k} = (-1)^i \binom{n-1}{i} \tag{5.5.5}$$

and the sum obtained by summing by the top index in the binomial instead of the bottom,

$$\sum_{n=0}^{i} \binom{n}{k} = \binom{i+1}{k+1}. \tag{5.5.6}$$

Both can be proved easily by induction using the identity

$$\binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k+1}. \tag{5.5.7}$$

The second sum is useful as another way of summing powers of integers. For example, from

$$n^2 = 2\binom{n}{2} + \binom{n}{1}, \tag{5.5.8}$$

it follows that

$$\sum_{n=0}^{i} n^2 = 2\binom{i+1}{3} + \binom{i+1}{2} = \frac{1}{6}i(i+1)(2i+1). \tag{5.5.9}$$

In the computation of the expected value of three independent Bernoulli random variables, N. Calkin [**88**] needed an expression for the sum of $A_{n,i}^3$. His approach to this question is illustrated first in a simple example.

Proposition 5.5.4. *For $n \in \mathbb{N}$,*

$$\sum_{i=0}^{n} A_{n,i} = (n+2)2^{n-1}.$$

Proof. The identity

$$A_{n,i} + A_{n,n-i} = 2^n + \binom{n}{i} \tag{5.5.10}$$

is summed from $i = 0$ to n. This gives the result. □

Exercise 5.5.5. Establish the identity

$$\sum_{i=0}^{n} \binom{n}{i} A_{n,i} = 2^{2n-1} + \frac{1}{2}\binom{2n}{n}.$$

N. Calkin's result is stated next.

Theorem 5.5.6. *Let $n \in \mathbb{N}$. Then*

$$\sum_{i=0}^{n} A_{n,i}^3 = n2^{3n-1} + 2^{3n} - 3n2^{n-2}\binom{2n}{n}. \tag{5.5.11}$$

The proof is based on the fact that the left-hand side, denoted by f_n, satisfies the linear recurrence

$$f_{n+1} - 8f_n = 4 \cdot 2^{3n} - 3 \cdot 2^n \binom{2n}{n}. \tag{5.5.12}$$

Solving this recurrence gives (5.5.11). The proof begins with some preliminary results.

Lemma 5.5.7. *For $n \in \mathbb{N}$,*

$$\sum_{i=0}^{n} A_{n,i}\binom{n}{i}^2 = 2^{n-1}\binom{2n}{n} + \frac{1}{2}\sum_{i=0}^{n}\binom{n}{i}^3.$$

Proof. The symmetry of the binomial coefficients gives

$$\sum_{i=0}^{n} A_{n,i}\binom{n}{i}^2 = \sum_{i=0}^{n} A_{n,n-i}\binom{n}{i}^2.$$

Now compute the average of these two formulas and use (5.5.10) to produce

$$\begin{aligned}\sum_{i=0}^{n} A_{n,i}\binom{n}{i}^2 &= \frac{1}{2}\sum_{i=0}^{n}\left(2^n + \binom{n}{i}\right)\binom{n}{i}^2 \\ &= 2^{n-1}\sum_{i=0}^{n}\binom{n}{i}^2 + \frac{1}{2}\sum_{i=0}^{n}\binom{n}{i}^3.\end{aligned}$$

This gives the result. □

Lemma 5.5.8. *Let $n \in \mathbb{N}$. Then*

$$\sum_{i=0}^{n} A_{n,i}^2\binom{n}{i} = \frac{1}{3}2^{3n} + 2^{n-1}\binom{2n}{n} + \frac{1}{6}\sum_{i=0}^{n}\binom{n}{i}^3.$$

Proof. The proof employs Lemma 5.5.7 in the expansion

$$\begin{aligned} A_{n,n}^3 &= \sum_{i=0}^{n} \left(A_{n,i}^3 - A_{n,i-1}^3 \right) = \sum_{i=0}^{n} \left[A_{n,i}^3 - \left(A_{n,i} - \binom{n}{i} \right)^3 \right] \\ &= 3\sum_{i=0}^{n} A_{n,i}^2 \binom{n}{i} - 3 \cdot 2^{n-1} \binom{2n}{n} - \frac{1}{2} \sum_{i=0}^{n} \binom{n}{i}^3 . \end{aligned}$$

The value $A_{n,n} = 2^n$ gives the result. □

Lemma 5.5.9. *The sum f_n satisfies the recurrence* (5.5.12).

Proof. Start with

$$\begin{aligned} f_{n+1} &= \sum_{i=0}^{n+1} \left(\sum_{k=0}^{i} \binom{n+1}{k} \right)^3 \\ &= \left(\sum_{k=0}^{n+1} \binom{n+1}{k} \right)^3 + \sum_{i=0}^{n} \left(\sum_{k=0}^{i} \binom{n+1}{k} \right)^3 \\ &= 2^{3n+3} + \sum_{i=0}^{n} \left(\sum_{k=0}^{i} \binom{n}{k} + \binom{n}{k-1} \right)^3 \\ &= 2^{3n+3} + \sum_{i=0}^{n} \left(2A_{n,i} - \binom{n}{i} \right)^3 . \end{aligned}$$

Expanding the last term yields

$$f_{n+1} = 2^{3n+3} + 8\sum_{i=0}^{n} A_{n,i}^3 - 12\sum_{i=0}^{n} A_{n,i}^2 \binom{n}{i} + 6\sum_{i=0}^{n} A_{n,i} \binom{n}{i}^2 - \sum_{i=0}^{n} \binom{n}{i}^3 .$$

Replacing the values from Lemma 5.5.7 and Lemma 5.5.8 gives the result. □

Note 5.5.10. Another problem involving sums of cubes of binomial coefficients was proposed by P. Barrucand [**40**]. Let

$$Y_n = \sum_{i+j+k=n} \frac{n!^2}{i!^2\, j!^2\, k!^2} \tag{5.5.13}$$

be the sums of squares of trinomial coefficients of rank n, defined in (2.11.1). The identity stated in [**40**] is

$$Y_n = \sum_{i=0}^{n} \binom{n}{i} L_3(i),$$

with $L_3(i)$ the sum of cubes of binomial coefficients, defined in (5.1.5). One of the solutions to Barrucand's problem involves the equivalent formulation

$$\sum_{k=0}^{n} \binom{n}{k} \sum_{j=0}^{k} \binom{k}{j}^3 = \sum_{k=0}^{n} \binom{n}{k}^2 \binom{2k}{k}.$$

In turn, this can be expressed in terms of exponential generating functions as

$$\sum_{n=0}^{\infty} Y_n \frac{x^n}{n!} = e^x \sum_{n=0}^{\infty} L_3(n) \frac{x^n}{n!}.$$

Exercise 5.5.11. Verify that the numbers Y_n satisfy the recurrence

$$(n+1)^2 Y_{n+1} = (10n^2+10n+3)Y_n - 9n^2 Y_{n-1}.$$

Examine arithmetic properties of these integers. For instance, Y_n is always divisible by 3. Experimental data suggests that Y_n is not divisble by the primes 2, 7, 13, 37, 61, 73.

Exercise 5.5.12. Find other examples of integers a, b such that

$$\sum_{k=0}^{n} \binom{n}{k} \sum_{j=0}^{k} \binom{k}{j}^a = \sum_{k=0}^{n} \binom{n}{k}^b \binom{2k}{k}.$$

Note 5.5.13. M. Hirschhorn [**169**] has provided systematic proofs of the evaluations of these sums. W. Y. C. Chen and collaborators [**97**] have developed an automatic procedure, named the **Abel-Zeilberger algorithm**. This provides automatic proofs of the identities

$$\begin{aligned}
\sum_{i=0}^{n} A_{n,i} &= (n+2)2^{n-1}, \\
\sum_{i=0}^{n} A_{n,i}^2 &= (n+2)2^{2n-1} - \frac{n}{2}\binom{2n}{n}, \\
\sum_{i=0}^{n} A_{n,i}^3 &= n2^{3n-1} + 2^{3n} - 3n2^{n-2}\binom{2n}{n}.
\end{aligned}$$

Chapter 6

Catalan Numbers

6.1. The placing of parentheses

The formation of an algebraic formula requires that symbols are separated by parentheses to indicate the order of operations. The rules indicate that, if reading these parentheses from left to right, the number of left parentheses (must be at least the number of right parentheses) . In any formula, the number of symbols of each type must be the same. This leads to a natural counting exercise:

Given $2n$ symbols, n of type (and n of type) , count the number of ways to arrange them in such a way that, when reading from left to right, the number of ('s is at least the number of) 's.

The number of ways to do this is called the **Catalan number**, denoted here by C_n. For $n = 0$, this definition is extended by $C_0 = 1$.

6.2. A recurrence

The definition of C_n given earlier implies that there are $2n$ symbols consisting of n open parentheses and n closed ones. Assume that the closing of the first open parenthesis is such that it contains $2k$ symbols in between. Therefore the distribution of symbols has the form

$$(\;\; 2k \text{ symbols } \;\;) \quad \text{followed by } 2n-2k-2 \text{ symbols.} \tag{6.2.1}$$

For example

$$(\; (\; (\;) \;) \; (\;) \;) \; (\; (\;) \;)$$

has $n = 6$ and $k = 3$.

This formulation of the placing of parentheses leads to a recurrence for the sequence C_n.

Theorem 6.2.1. *The Catalan numbers C_n satisfy the recurrence*

$$C_n = \sum_{k=0}^{n-1} C_k C_{n-1-k} \tag{6.2.2}$$

for $n \geq 1$.

The recurrence provides the first few values

$$C_0 = 1,\; C_1 = 1,\; C_2 = 2,\; C_3 = 5,\; C_4 = 14,\; C_5 = 42,\; C_6 = 132.$$

The next exercise provides a second combinatorial description of the Catalan numbers. The reader will find a very large number of these interpretations in the first volume of R. Stanley's treatise [**279**] and in its second edition [**280**]. The next couple of exercises provide two of them.

Exercise 6.2.2. Consider paths of length $2n$ on the lattice $\mathbb{Z} \times \mathbb{Z}$ starting at the origin $(0, 0)$ and ending on the horizontal axis. The steps are of the form $NE : (i, j) \mapsto (i + 1, j + 1)$, or $SW : (i, j) \mapsto (i - 1, j - 1)$. Prove that C_n counts the number of such paths that remain above the x-axis. **Hint:** Replace a left (right) parenthesis by a NE (SW) step.

Exercise 6.2.3. Prove that C_n counts the number of binary trees with n nodes. A **binary tree** is one where every vertex has no children, a left child, a right child, or both.

6.3. The generating function

The recurrence (6.2.2) is now employed to obtain an analytic expression for the generating function

$$Ca(x) = \sum_{n=0}^{\infty} C_n x^n. \tag{6.3.1}$$

Theorem 6.3.1. *The generating function for the Catalan numbers is given by*

$$Ca(x) = \frac{1-\sqrt{1-4x}}{2x} = \frac{2}{1+\sqrt{1-4x}}. \tag{6.3.2}$$

In particular, $y = Ca(x)$ *satisfies* $xy^2 - y + 1 = 0$*, so it is an algebraic function of* x*.*

Proof. Squaring (6.3.2) gives

$$\begin{aligned} Ca^2(x) &= \sum_{j=0}^{\infty} C_j x^j \times \sum_{k=0}^{\infty} C_k x^k \\ &= \sum_{j,k\geq 0} C_j C_k x^{j+k}. \end{aligned}$$

Now let $\nu = j+k$ and sum over all possible values. Then the new index ν ranges over $\mathbb{N}_0$ and, for fixed ν, the index j varies over $0 \leq j \leq \nu$. Therefore

$$Ca^2(x) = \sum_{\nu=0}^{\infty} \left(\sum_{j=0}^{\nu} C_j C_{\nu-j} \right) x^{\nu}. \tag{6.3.3}$$

The recurrence in Theorem 6.2.1 shows that this can be written as

$$\begin{aligned} Ca^2(x) &= \sum_{\nu=0}^{\infty} C_{\nu+1} x^{\nu} \\ &= \frac{1}{x}(Ca(x) - 1). \end{aligned}$$

This gives the quadratic equation

$$xCa^2(x) - Ca(x) + 1 = 0 \tag{6.3.4}$$

with solutions

$$Ca(x) = \frac{1 \pm \sqrt{1-4x}}{2x}. \tag{6.3.5}$$

The value $C(0) = C_0 = 1$ shows that the minus sign is the correct one. □

An explicit formula. The generating function

$$Ca(x) = \sum_{n=0}^{\infty} C_n x^n = \frac{1-\sqrt{1-4x}}{2x} \tag{6.3.6}$$

is now employed to obtain an explicit formula for C_n.

Start with the generating function of the central binomial coefficients (2.7.5)

$$\sum_{n=0}^{\infty} \binom{2n}{n} x^n = \frac{1}{\sqrt{1-4x}} \tag{6.3.7}$$

and integrate to obtain

$$\sum_{n=0}^{\infty} \frac{1}{n+1}\binom{2n}{n} x^{n+1} + \alpha = -\frac{1}{2}\sqrt{1-4x}, \tag{6.3.8}$$

where α is a constant of integration. Replacing $x=0$ gives $\alpha = -1/2$.

Then

$$\begin{aligned} 2xCa(x) &= 1-\sqrt{1-4x} \\ &= 1+2\left(\sum_{n=0}^{\infty} \frac{1}{n+1}\binom{2n}{n} x^{n+1} - \frac{1}{2}\right) \\ &= 2\sum_{n=0}^{\infty} \frac{1}{n+1}\binom{2n}{n} x^{n+1}. \end{aligned}$$

This yields

$$Ca(x) = \sum_{n=0}^{\infty} \frac{1}{n+1}\binom{2n}{n} x^n, \tag{6.3.9}$$

which gives an expression for C_n.

Theorem 6.3.2. *The Catalan numbers are given by*

$$C_n = \frac{1}{n+1}\binom{2n}{n}. \tag{6.3.10}$$

This expression for the Catalan numbers can be used to provide a different proof of the formula for the generating function.

Exercise 6.3.3. It is possible to derive the generating function for C_n from (6.3.10). Check the details.

Exercise 6.3.4. The Catalan numbers C_n are positive integers because they count a legal placing of $2n$ parentheses. This also follows from the identity

$$C_n = \binom{2n}{n} - \binom{2n}{n-1}. \tag{6.3.11}$$

Check this formula.

Exercise 6.3.5. Use the explicit formula (6.3.10) for C_n to verify the recurrence

$$(n+2)C_{n+1} = 2(2n+1)C_n. \tag{6.3.12}$$

Conversely, check that this implies (6.3.10). Use it to check that the generating function $Ca(x)$ satisfies the differential equation

$$x(4x-1)\frac{dCa}{dx} + (2x-1)Ca + 1 = 0, \tag{6.3.13}$$

with initial condition $C(0) = 1$. Solve this equation to find the generating function (6.3.2).

The first number-theoretical consequence of Catalan numbers is presented next.

Corollary 6.3.6. *Let $n \in \mathbb{N}$. Then $n+1$ divides $\binom{2n}{n}$.*

Exercise 6.3.7. Give a direct proof.

Exercise 6.3.8. Describe the integers $n \in \mathbb{N}$ for which $(n+1)^2$ divides $\binom{2n}{n}$. This sequence starts with $\{5, 14, 27, 41, 44, 65, 76, 90\}$.

The next corollary is a reformulation of the fact that $n+1$ divides $\binom{2n}{n}$. Recall that, for a prime p, the function $s_p(n)$ is the sum of the digits of n written in base p.

Corollary 6.3.9. *Let $n \in \mathbb{N}$ and let p be a prime. Then*

$$s_p(n) + s_p(n+1) \geq s_p(2n) + 1. \tag{6.3.14}$$

Proof. The fact that $n+1$ divides $\binom{2n}{n}$ implies that for every prime p, the valuations must satisfy $\nu_p(n+1) \leq \nu_p\left(\binom{2n}{n}\right)$. The identity $n+1 = (n+1)!/n!$ and Legendre's formula (2.6.2) give the result. □

Exercise 6.3.10. Use the binomial theorem to prove the identity

$$\frac{(1-4x)^{-1/2} - 1}{2x} = \sum_{n=0}^{\infty} \binom{2n+1}{n} x^n. \tag{6.3.15}$$

The next identity was proposed as a problem by R. Breusch [**79**]. The solution presented here is due to M. T. L. Bizley [**55**].

Proposition 6.3.11. *The Catalan numbers C_n satisfy*

$$\sum_{i=0}^{n} \binom{2n-2i}{n-i} C_i = \binom{2n+1}{n}. \tag{6.3.16}$$

Proof. Observe that $\binom{2n-2i}{n-i}$ is the coefficient of x^{n-i} in the expansion of $(1-4x)^{-1/2}$. Thus the left-hand side is the coefficient of x^n in the expansion of $Ca(x)/\sqrt{1-4x}$, where $Ca(x)$ is the generating function of the Catalan numbers. The result now follows from Exercise 6.3.10 and the identity

$$\frac{Ca(x)}{\sqrt{1-4x}} = \frac{(1-4x)^{-1/2}-1}{2x}. \tag{6.3.17}$$

□

Among the many identities for Catalan numbers an important recurrence was established by J. Touchard [**292**]. The proof presented here is due to J. Riordan [**252**].

Theorem 6.3.12. *The Catalan numbers C_n satisfy*

$$C_{n+1} = \sum_{k=0}^{\lfloor n/2 \rfloor} \binom{n}{2k} 2^{n-2k} C_k. \tag{6.3.18}$$

Proof. Define $H_n(x)$ to be the generating function that enumerates the parentheses with n factors and k nests. Let $c_{n,k}$ be the coefficient of x^k in $H_n(x)$. The function $H_n(x)$ satisfies the recurrence

$$H_n(x) = H_1(x)H_{n-1}(x) + \cdots + H_j(x)H_{n-j}(x) + \cdots + H_{n-1}(x)H_1(x),$$

with initial conditions $H_1(x) = 1$ and $H_2(x) = x$. Introduce the notation

$$G(x,y) = \sum_{n=1}^{\infty} H_n(x)y^n.$$

The recurrence for H_n produces

$$\sum_{n=1}^{\infty} H_n(x)y^n = \sum_{n=1}^{\infty} H_1(x)H_{n-1}(x)y^n + \cdots + \sum_{n=1}^{\infty} H_j(x)H_{n-j}(x)y^n$$
$$+ \cdots + \sum_{n=1}^{\infty} H_{n-1}(x)H_1(x)y^n.$$

Exercise 6.3.13. Check that the previous relation yields

$$G(x,y) = y + (x-1)y^2 + G^2(x,y). \tag{6.3.19}$$

Conclude that

$$G(x,y) = \frac{1}{2}\left[1 - (1 - 4y - 4(x-1)y^2)^{1/2}\right]. \tag{6.3.20}$$

Prove that this can be written as

$$G(x,y) = (y + (x-1)y^2)C(y + (x-1)y^2), \tag{6.3.21}$$

where C is the generating function for the Catalan numbers.

Expanding (6.3.21) gives

$$H_n(x) = \sum_{k=0}^{\infty} \binom{n-k}{k} (x-1)^k C_{n-1-k}. \tag{6.3.22}$$

Now differentiate (6.3.20) to obtain

$$\begin{aligned} \left[1 - 2G(x,y)\right] G_x(x,y) &= y^2, \\ \left[1 - 2G(x,y)\right] G_y(x,y) &= 1 + 2(x-1)y, \end{aligned}$$

which gives

$$\left[1 + 2(x-1)y\right] G_x(x,y) = y^2 G_y(x,y). \tag{6.3.23}$$

Replace the expansion of $G(x,y)$ to produce

$$H_n'(x) + 2(x-1)H_{n-1}'(x) = (n-1)H_{n-1}(x). \tag{6.3.24}$$

This leads to the recurrence

$$kc_{n,k} = 2kc_{n-1,k} + (n+1-2k)c_{n-1,k-1}. \tag{6.3.25}$$

Use the initial values

$$c_{n,0} = \delta_{n,1} = \begin{cases} 1 & \text{if } n = 0, \\ 0 & \text{otherwise} \end{cases}$$

and $c_{n,1} = 2^{n-2}$ and $c_{n,2} = \binom{n-2}{2}2^{n-4}$ to obtain the expression

$$c_{n,k} = \binom{n-2}{2k-2} 2^{n-2k} C_{k-1}. \tag{6.3.26}$$

It follows that

$$H_n(x) = \sum_{k=1}^{m} \binom{n-2}{2k-2} 2^{n-2k} C_{k-1} x^k, \tag{6.3.27}$$

with $m = \left\lfloor \frac{n}{2} \right\rfloor$. In particular,

$$C_{n+1} = H_{n+2}(1) = \sum_{k=1}^{m} \binom{n}{2k} 2^{n-2k} C_k, \tag{6.3.28}$$

as claimed. □

6.4. Arithmetical properties

This section discusses arithmetical properties of Catalan numbers C_n. The first exercise is elementary.

Exercise 6.4.1. Prove that C_n is prime only for $C_3 = 5$. **Hint:** Every prime divisor p of C_n satisfies $p \leq 2n$.

The next question of interest is to describe the p-adic valuations of C_n. The next exercise provides a simple argument that determines the 2-adic valuation of C_n.

Exercise 6.4.2. Show that

$$\nu_2(C_n) = s_2(n) - \nu_2(n+1), \tag{6.4.1}$$

where $s_2(n)$ is the number of ones in the binary expansion of n. Conclude that if n is even, then so is C_n and

$$\nu_2(C_{2n}) = s_2(n).$$

The discussion for odd indices is more elaborate. The indices for which $\nu_2(C_n) = 0$ are simple to determine.

Theorem 6.4.3. *The number C_n is odd if and only if $n+1$ is a power of 2.*

Proof. If $n+1=2^r$, then $n=1+2+2^2+\cdots+2^{r-1}$ and $s_2(n)=r$. The result follows from (6.4.1). To verify the converse, write $n+1=2^r m$ with m odd. Then

$$m=1+a_1 2+a_2 2^2+\cdots+a_t 2^t \tag{6.4.2}$$

implies that

$$n+1=2^r m=2^r+\cdots+a_t\cdot 2^{r+t} \tag{6.4.3}$$

and

$$n=2^r-1+a_1\cdot 2^{r+1}+\cdots+a_t\cdot 2^{r+t}. \tag{6.4.4}$$

Therefore

$$s_2(n)=r+a_1+a_2+\cdots+a_t. \tag{6.4.5}$$

The condition $s_2(n)=\nu_2(n+1)=r$ implies $a_1=a_2=\cdots=a_t=0$. That is, $m=1$ and $n+1=2^r$, as claimed. □

Exercise 6.4.4. For fixed $j\in\mathbb{N}$, characterize the indices n for which $\nu_2(C_n)=j$. The table of values of $\nu_2(C_n)$, for $n\geq 1$, begins as

$$\{0,\,1,\,0,\,1,\,1,\,2,\,0,\,1,\,1,\,2,\,1,\,2,\,2,\,3,\,0,\,1\}$$

so, for instance, the list of indices n for which $\nu_2(C_n)=2$ starts as

$$\{6,\,10,\,12,\,13,\,18,\,20,\,21,\,24,\,25,\,27,\,34,\,36,\,37,\,40,\,41,\,43,\,48,\,49\}.$$

Figure 6.4.1 shows the values of this list up to $n\leq 500000$.

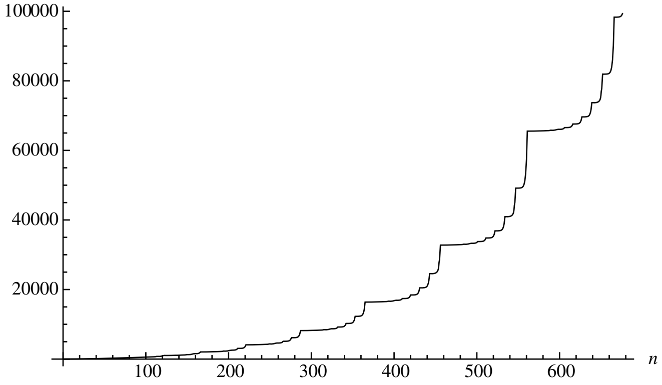


Figure 6.4.1. Indices where the 2-adic valuation of C_n is 2.

Proof. The second proof of Theorem 6.4.3 is combinatorial. (The author wishes to thank B. Sagan for providing the argument.) Assume that $n = 2^k - 1$ and recall from Exercise 6.2.3 that C_n counts binary trees with n nodes. Note that the tree T_k which has all of its leaves at depth k has $n = 2^k - 1$ nodes (the depth of a vertex v being the number of nodes on the path from the root to v). If T is not T_k, then there must be some vertex v in T such that the left and right subtrees of v are not isomorphic. Among all such v, consider those at the greatest depth, and among those pick the one which is leftmost. Map T to T' where T' is obtained by interchanging the left and right subtrees of v. This map is clearly an involution since the choice of v makes one choose the same vertex when applying the map to T'. All trees except T_k have been paired up. This completes the argument. □

Note 6.4.5. A partial combinatorial argument of the general result (6.4.1) appears in the paper by E. Deutsch and B. Sagan [**110**].

Exercise 6.4.6. This exercise further explores properties of the function $\nu_2(C_n)$. The data begins with

$$\nu_2(C_n) = \{0,\, 0,\, 1,\, 0,\, 1,\, 1,\, 2,\, 0,\, 1,\, 1,\, 2,\, 1,\, 2,\, 2,\, 3,\, 0,\, 1,\, 1\}.$$

Now partition the positive integers $\mathbb{N}$ into blocks of length 7 defined by

$$\mathfrak{c}_n = \{\nu_2(C_j) : \, 8n \leq j \leq 8n + 6\},$$

plus the sequence of indices $j \equiv 7 \bmod 8$. Then

$$\mathfrak{c}_0 = \{0,\, 0,\, 1,\, 0,\, 1,\, 1,\, 2\}$$

and

$$\mathfrak{c}_1 = \{1,\, 1,\, 2,\, 1,\, 2,\, 2,\, 3\}$$

have the property that $\mathfrak{c}_1 - \mathfrak{c}_0$ is a constant sequence (consisting of all 1's). This property seems to extend to all $n \in \mathbb{N}$. Define

$$y_n := \text{ the common term in the sequence } \mathfrak{c}_n - \mathfrak{c}_0.$$

The exercise requests a proof that the sequence $\{y_n : \, n \in \mathbb{N}\}$ is given by $1+\nu_2(C_n)$. On the other hand, the sequence of indices $j \equiv 7 \bmod 8$ satisfies

$$\nu_2(C_{8n+7}) = \nu_2(C_n). \tag{6.4.6}$$

It would be interesting to have an explanation of this phenomenon.

Exercise 6.4.7. Let p be a prime. Define the numbers a_k by the expansion

$$n+1=\sum_{k=0}^{r} a_k p^k.$$

Prove that

$$\nu_2(C_n)=|\{a_k=1\}|-1,$$

and for $p>2$

$$\nu_p(C_n)=\left|\left\{a_k>\tfrac{1}{2}(p+1)\right\}\right|-1.$$

Hint: Use Kummer's formula in Theorem 2.6.7.

Exercise 6.4.8. This exercise outlines some properties of the 3-adic valuation of Catalan numbers. Prove first that

$$\nu_3(C_{3n-1})=\nu_3(C_{3n})=\nu_3(C_{3n+1}).$$

Therefore, $\nu_3(C_n)$ is determined by the function $f(n):=\nu_3(C_{3n})$. Show that

$$f(3n)=f(3n+1)=f(n),$$

which leaves $f(3n+2)$ for consideration. The sequence $3n+2$ splits modulo 9 into $9n+2$, $9n+5$, and $9n+8$. Prove that

$$f(9n+2)=f(n)+1,$$

$$f(9n+5)=f(3n+2)+1,$$

and

$$f(9n+8)=f(3n+2)+1.$$

Conclude that every sequence of the form $\{\nu_3(C_{3^a n+b}):\, n\in\mathbb{N}\}$, with $n\in\mathbb{N}$ and $0\leq b<3^a$, is a linear combination of the sequences $\nu_3(3n)$ and $\nu_3(C_{3n+2})$. This states that the sequence $\nu_3(C_n)$ is 3-regular in the sense of Note 3.5.14. Describe this result in terms of a valuation tree.

6.5. An integral expression

The **Hausdorff moment problem** asks for necessary and sufficient conditions on the numbers μ_n in order that there exists a distribution function Φ on $[0,1]$ such that

$$\mu_n = \int_0^1 x^n d\Phi(x) \tag{6.5.1}$$

for all $n \in \mathbb{N}_0$. The reader can think of Φ in the form $\varphi(x)\,dx$. The first example of the function φ appeared in Exercise 2.11.10 in the case of the central binomial coefficients. The corresponding solution for the Catalan numbers appeared in the paper by K. A. Penson and J.-M. Sixdeniers [**245**]. This example connects Catalan numbers to Wallis' formula, one of the earliest integral evaluations.

Theorem 6.5.1. *The function*

$$\varphi(x) = \frac{1}{\pi}\sqrt{\frac{1-x}{x}} \tag{6.5.2}$$

satisfies

$$Z_n := \int_0^1 x^n \varphi(x)\,dx = \frac{C_n}{2^{2n+1}}. \tag{6.5.3}$$

Proof. The change of variables $x = \cos^2 t$ yields

$$Z_n = \frac{2}{\pi}\int_0^{\pi/2} \cos^{2n} t\,\sin^2 t\,dt. \tag{6.5.4}$$

Introduce the notation

$$W_n = \int_0^{\pi/2} \cos^{2n} t\,dt \tag{6.5.5}$$

to write the previous step as

$$Z_n = \frac{2^{2n+2}}{\pi}\left(W_n - W_{n+1}\right). \tag{6.5.6}$$

The result now follows from **Wallis' formula**:

$$W_n = \frac{\pi}{2^{2n+1}}\binom{2n}{n}. \tag{6.5.7}$$

Chapter 9 is dedicated to the many proofs of (6.5.7) available in the literature. □

Chapter 7

The Stirling Numbers of the Second Kind

7.1. Introduction

This chapter considers the **Stirling numbers of the second kind** with special emphasis on their arithmetic properties. The other kind of Stirling numbers, those of the first kind, are not considered here.

Definition 7.1.1. Let n, $k \geq 1$. The **Stirling numbers of the second kind** $S(n,k)$ count the ways to divide a set of n objects into k nonempty subsets.

Note 7.1.2. From the definition it is clear that $S(n,k) = 0$ if $n < k$. The extension

$$S(0,k) = \begin{cases} 1 & \text{if } k = 0, \\ 0 & \text{if } k > 0 \end{cases}$$

defines $S(0,k)$.

Example 7.1.3. The number $S(n,1) = 1$ since the only option is to place all the objects into the single subset. Similarly, $S(n,n) = 1$ since then you must place each object in a different subset.

Example 7.1.4. The list

$$\{\{1,2,3\},\{4\}\},\ \ \{\{1,2,4\},\{3\}\},\ \ \{\{1,3,4\},\{2\}\},\ \ \{\{2,3,4\},\{1\}\},$$
$$\{\{1,2\},\{3,4\}\},\ \ \{\{1,3\},\{2,4\}\},\ \ \{\{1,4\},\{2,3\}\}$$

shows that $S(4,2) = 7$.

Exercise 7.1.5. Give a combinatorial proof of the value

$$S(n,n-1) = \binom{n}{2}. \tag{7.1.1}$$

Exercise 7.1.6. Prove that

$$S(n,2) = 2^{n-1} - 1. \tag{7.1.2}$$

7.2. A recurrence

In the partition of $\{1,\ 2,\ \ldots,\ n\}$ into k nonempty subsets, there are cases in which n appears as a singleton and others in which n is part of one of the k nonempty subsets with more than one element. In the first case, the partition is $\{n\}$ together with a partition of $\{1,\ 2,\ \ldots,\ n-1\}$ into $k-1$ nonempty parts. There are $S(n-1,k-1)$ of them. In the second case, taking n out of the partition yields a collection of k nonempty subsets partitioning $\{1,\ 2,\ \ldots,\ n-1\}$. There are $S(n-1,k)$ of them. The number n can be placed back into any of the k parts. This proves the next result.

Theorem 7.2.1. *The Stirling numbers of the second kind satisfy the recurrence*

$$S(n,k) = S(n-1,k-1) + kS(n-1,k) \tag{7.2.1}$$

for $n \geq 2$.

Exercise 7.2.2. The theorem and $S(n,1) = n$ state that

$$S(n,2) - 2S(n-1,2) = S(n-1,1) = 1. \tag{7.2.2}$$

Solve this recurrence to confirm the value $S(n,2) = 2^{n-1} - 1$ stated in Exercise 7.1.6. Discuss the consistency of the value $S(0,k)$ and this recurrence.

Exercise 7.2.3. Let $f(x) = 1/(1+e^x)$. Prove that

$$f^{(n)}(x) = \sum_{k=1}^{n+1} \frac{a(n,k)}{(1+e^x)^k} \tag{7.2.3}$$

where

$$a(n,k) = (-1)^{n+k+1}(k-1)!S(n+1,k). \tag{7.2.4}$$

Hint: Differentiate (7.2.3) to obtain a recurrence for $a(n,k)$.

Exercise 7.2.4. Use the recurrence (7.2.1) to establish the generating function

$$\sum_{n=0}^{\infty} S(n,k)x^n = \frac{x^k}{(1-x)(1-2x)(1-3x)\cdots(1-kx)} \tag{7.2.5}$$

for the Stirling numbers $S(n,k)$.

Exercise 7.2.5. Iterate the recurrence (7.2.1) to obtain the identity

$$S(n+j,k) = \sum_{i=0}^{j} p_{j,i}(k)S(n,k-j+i)$$

where the $p_{j,i}(k)$ are polynomials in k of degree i that satisfy the recurrence

$$p_{j+1,i}(k) = p_{j,i}(k) + (k-j+i-1)p_{j,i-1}(k)$$

and have the initial conditions $p_{j,0}(k) = 1$ and $p_{j,j}(k) = k^j$. Write the polynomials $p_{j,i}$ in terms of the falling factorials

$$(k)_r = k(k-1)\cdots(k-r+1),$$

in the form

$$p_{j,i}(k) = \sum_{r=0}^{i} c_{j,i}(r)(k)_r,$$

and check the recurrence

$$c_{j+1,i}(r) = c_{j,i}(r) + (r-j+i-1)c_{j,i-1}(r) + c_{j,i-1}(r).$$

The next theorem presents a combinatorial proof of a different type of recurrence satisfied by the Stirling numbers.

Theorem 7.2.6. *The Stirling numbers $S(n,k)$ satisfy the recurrence*

$$k!S(n,k) = k^n - \sum_{i=1}^{k-1} k(k-1)\cdots(k-i+1)S(n,i). \tag{7.2.6}$$

Proof. Suppose there are n balls (numbered 1 to n) and k boxes (numbered 1 to k). Let $t(n,k)$ be the number of ways to place the n balls into the k boxes in such a way that no box is empty. Then $t(n,k) = k!S(n,k)$ and $t(n,1) = 1$. Think about this. Assume that $t(n,1), \ldots, t(n,k-1)$ is known. There are k^n ways to place the n balls into the k boxes if the requirement that no box should be empty is dropped. Now, for each i in the range $1 \leq i \leq k-1$, there are $\binom{k}{i}$ configurations for which exactly i boxes are empty, and for each such configuration, there are $t(n,k-i)$ ways to place the n balls into the other $k-i$ boxes. Then

$$t(n,k) = k^n - \sum_{i=1}^{k-1} \binom{k}{i} t(n,k-1).$$

Multiply by $k!$ to get the stated recurrence. □

Exercise 7.2.7. Use (7.2.6) to confirm the value $S(n,2) = 2^{n-1} - 1$ given as Exercise 7.1.6.

7.3. An explicit formula

This section produces an explicit formula for $S(n,k)$. The proofs employ the ***inclusion-exclusion principle***. A short explanation is presented first. Consider a collection of sets $\{A_j : 1 \leq j \leq n\}$ and denote the cardinality of A_j by $|A_j|$. If the sets are disjoint, that is, $A_i \cap A_j = \emptyset$ for $i \neq j$, then

$$\left| \bigcup_{j=1}^{n} A_j \right| = \sum_{j=1}^{n} |A_j|. \tag{7.3.1}$$

The proof is clear: every element in the union of the sets belongs to a unique set A_j. Thus, in (7.3.1), every element is counted exactly once. The inclusion-exclusion principle, stated below, describes how to count unions in case the sets have elements in common.

Theorem 7.3.1. *Let* $\{A_j : 1 \leq j \leq n\}$ *be a collection of sets. Then*

$$\begin{aligned} \left| \bigcup_{j=1}^{n} A_j \right| &= \sum_{i_1} |A_{i_1}| - \sum_{i_1<i_2} |A_{i_1} \cap A_{i_2}| + \sum_{i_1<i_2<i_3} |A_{i_1} \cap A_{i_2} \cap A_{i_3}| \\ &\quad + \cdots + (-1)^{n-1} |A_1 \cap A_2 \cap \cdots A_n|, \end{aligned}$$

where the indices i_k *run over* $\{1, \ldots, n\}$.

Proof. Assume x is an element in the union of the sets A_i. Let k be the number of sets A_i that contain x. It may be assumed that x is in the sets $A_1, A_2, \ldots, A_k$. The element x contributes 1 to the count on the left. Its contribution to the right is

$$k - \binom{k}{2} + \binom{k}{3} - \cdots + (-1)^{k-1}\binom{k}{k} = \sum_{j=1}^{k} (-1)^{j-1} \binom{k}{j}. \tag{7.3.2}$$

The binomial theorem gives

$$\sum_{j=0}^{k} (-1)^j \binom{k}{j} = (1-1)^k = 0. \tag{7.3.3}$$

This gives

$$\sum_{j=1}^{k} (-1)^{j-1} \binom{k}{j} = -\sum_{j=0}^{k} (-1)^j \binom{k}{j} + 1 = 1.$$

The formula has been established. □

The next theorem produces a closed-form formula for $S(n,k)$.

Theorem 7.3.2. *The Stirling numbers of the second kind are given by*

$$S(n,k) = \frac{1}{k!} \sum_{j=0}^{k-1} (-1)^j \binom{k}{j} (k-j)^n. \tag{7.3.4}$$

Proof. The proof is obtained by counting in two different forms the number of functions from $A = \{1, 2, \ldots, n\}$ onto $B = \{1, 2, \ldots, k\}$. The first form involves the Stirling numbers and the second form employs the inclusion-exclusion principle.

To produce an onto function f, partition the set A into k disjoint nonempty parts C_i and then define f by $f(x) = i$ for $x \in C_i$. This can be done in $S(n,k)$ ways. Each such partition generates $k! \times S(n,k)$ onto functions by permuting the k sets C_i. It is clear that every onto function must be of this form. It follows that

$$|f : A \to B \text{ that are onto }| = k! \times S(n,k). \tag{7.3.5}$$

Observe that this statement is also valid for $k > n$, since both sides vanish in this case.

The inclusion-exclusion principle is now employed to produce a second count of the onto functions $f : A \to B$. Let X be the set of all functions $f : A \to B$. It is clear that $|X| = k^n$. The value of the image for each element in A has exactly k choices. Now, for each i in the range $1 \leq i \leq k$, define

$$X_i = \{f : A \to B : f \text{ omits } i \text{ in its range.}\}. \tag{7.3.6}$$

Then

$$\begin{aligned} |f : A \to B \text{ that are onto }| &= \left| \bigcap_{i=1}^{k} (X - X_i) \right| \\ &= \left| X - \bigcup_{i=1}^{k} X_i \right| \\ &= k^n - \left| \bigcup_{i=1}^{k} X_i \right| . \end{aligned}$$

Now, with the notation $[n] = \{1, 2, \ldots, n\}$, observe that

$$|X_i| = |\{f : [n] \to [k-1]\}| = (k-1)^n.$$

Similarly

$$|X_{i_1} \cap X_{i_2} \cap \cdots \cap X_{i_j}| = |\{f : [n] \to [k-j]\}| = \binom{k}{j}(k-j)^n.$$

The inclusion-exclusion principle gives

$$\begin{aligned} |f : A \to B \text{ that are onto }| &= k^n - \left(\sum_{j=1}^{k} (-1)^{j-1} \binom{k}{j} (k-j)^n \right) \\ &= \sum_{j=0}^{k} (-1)^j \binom{k}{j} (k-j)^n . \end{aligned}$$

Comparing both computations gives the result. □

Exercise 7.3.3. Confirm the values

$$S(n,3) = \frac{1}{2}(3^{n-1} - 2^n + 1) \tag{7.3.7}$$

and

$$S(n,4) = \frac{1}{6}(3 \cdot 2^{n-1} - 3^n + 2^{2n-2} - 1). \tag{7.3.8}$$

Exercise 7.3.4. Use the result of Theorem 7.3.2 to check that the numbers $a(n,k)$ in Exercise 7.2.3 can be written as

$$a(n,k) = (-1)^n \sum_{j=0}^{k-1} (-1)^j \binom{k-1}{j} (j+1)^n. \tag{7.3.9}$$

7.4. The valuations of Stirling numbers

This section discusses the sequence $\{\nu_2(S(n,k)) : n \geq k\}$ for k fixed. The cases $k = 1$, 2 are elementary since $S(n,1) = 1$ and $S(n,2) = 2^n - 1$. Therefore $\nu_2(S(n,k)) = 0$ for these values of k.

The next theorem deals with $k = 3$.

Theorem 7.4.1. *The* 2*-adic valuations of the Stirling numbers of order* 3

$$S(n,3) = \frac{1}{2}(3^{n-1} - 2^n + 1), \quad \textit{for } n \geq 3, \tag{7.4.1}$$

are given by

$$\nu_2(S(n,3)) = \begin{cases} 0 & \textit{if } n \textit{ is odd,} \\ 1 & \textit{if } n \textit{ is even.} \end{cases} \tag{7.4.2}$$

Proof. The explicit formula comes from Exercise 7.3.3. Iterate the recurrence

$$S(n,3) = S(n-1,2) + 3S(n-1,3) \tag{7.4.3}$$

to produce

$$S(n,3) = 2^{n-2} - 1 + \sum_{k=1}^{n-3} 3^k (2^{n-k-2} - 1), \qquad \text{for } n \geq 3. \tag{7.4.4}$$

This shows that if n is odd, then $S(n,3)$ is odd. Thus $\nu_2(S(n,3)) = 0$.

To treat the case of n even, iterate (7.4.3) to obtain

$$S(n,3) = 2^{n-2} + 3 \cdot 2^{n-3} - 4 + 9S(n-2,3). \tag{7.4.5}$$

As an inductive step write $S(n-2,3) = 2T_{n-2}$ with T_{n-2} odd. Then

$$\frac{1}{2}S(n,3) = 2^{n-3} + 3 \cdot 2^{n-4} - 2 + 9T_{n-2} \tag{7.4.6}$$

is an odd integer. This completes the induction. □

The case of $k = 4$ can be decided in a similar manner.

Theorem 7.4.2. *The Stirling numbers of order* 4

$$S(n,4) = \frac{1}{6}(4^{n-1} - 3^n + 3 \cdot 2^{n-1} - 1) \tag{7.4.7}$$

satisfy

$$\nu_2(S(n,4)) = 1 - \nu_2(S(n,3)) = \begin{cases} 1 & \textit{if } n \textit{ is odd,} \\ 0 & \textit{if } n \textit{ is even.} \end{cases} \tag{7.4.8}$$

Proof. The expression for $S(n,4)$ comes from Theorem 7.3.2. The recurrence (7.2.1) gives

$$S(n,4) = S(n-1,3) + 4S(n-1,4). \tag{7.4.9}$$

For n even, the value $S(n-1,3)$ is odd, so that $S(n,4)$ is odd. Therefore $\nu_2(S(n,4)) = 0$. For n odd, $S(n,4)$ is even since $S(n-1,3)$ is even. The relation (7.4.9) is now written as

$$\frac{1}{2}S(n,4) = \frac{1}{2}S(n-1,3) + 2S(n-1,4). \tag{7.4.10}$$

The value $\nu_2(S(n-1,3)) = 1$ shows that the right-hand side is odd, yielding $\nu_2(S(n,4)) = 1$. □

7.4.1. The valuation of $S(n,5)$. The first nontrivial case occurs when $k = 5$. The sequence of values for $\nu_2(S(n,5))$ is computed by the formula

$$S(n,5) = \frac{1}{24}(5^{n-1} - 4^n + 2 \cdot 3^n - 2^{n+1} + 1), \quad n \geq 5, \tag{7.4.11}$$

coming from Theorem 7.3.2 or using the recurrence

$$S(n,5) = S(n-1,4) + 5S(n-1,5). \tag{7.4.12}$$

The first few values of $\nu_2(S(n,5))$ are given by

$$\nu_2(S(n,5)) = \{0,\ 0,\ 2,\ 1,\ 0,\ 0,\ 1,\ 3,\ 0,\ 0,\ 3,\ 1,\ 0,\ 0,\ 1,\ 2\},$$

and the pattern, shown in Figure 7.4.1, is now not easy to predict.

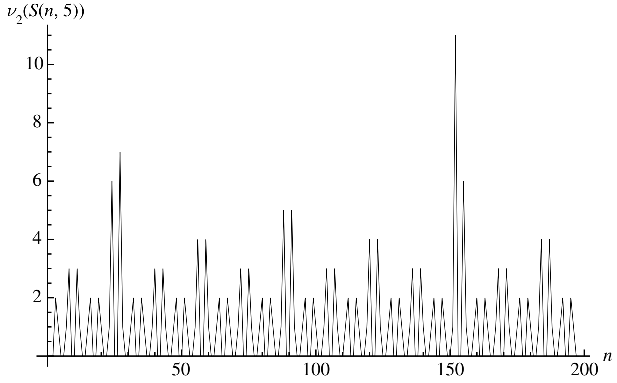


Figure 7.4.1. The 2-adic valuation of $S(n,5)$.

The analysis of the valuation $\nu_2(S(n,5))$ begins with some elementary observations.

Lemma 7.4.3. *The Stirling numbers $S(n,5)$ satisfy*

$$\nu_2(S(4n+1,5)) = \nu_2(S(4n+2,5)) = 0. \tag{7.4.13}$$

Proof. The recurrence (7.4.12) yields

$$\begin{aligned} S(4n+1,5) &= S(4n,4) + 5S(4n-1,4) + 5^2S(4n-2,4) \\ &\quad +5^3S(4n-3,4) + 5^4S(4n-3,5) \end{aligned}$$

and the result for $\nu_2(S(4n+1,5))$ follows by induction using the parity

$$S(n,4) \equiv \begin{cases} 1 \mod 2 & \text{if } n \equiv 0 \mod 2, \\ 0 \mod 2 & \text{if } n \equiv 1 \mod 2. \end{cases} \tag{7.4.14}$$

The case of $S(4n+2,5)$ is similar. □

It remains to describe $\nu_2(S(4n,5))$ and $\nu_2(S(4n+3,5))$. The first few values of $\nu_2(S(4n,5))$, for $n \geq 2$, are given by

$$\nu_2(S(4n,5)) = \{1,\ 3,\ 1,\ 2,\ 1,\ 6,\ 1,\ 2,\ 1,\ 3,\ 1,\ 2,\ 1,\ 4,\ 1,\ 2,\ 1,\ 3,\ 1\}.$$

The next step in the analysis of $\nu_2(S(n,5))$ is to show that every other entry in the values of $\nu_2(S(4n,5))$ is 1.

Lemma 7.4.4. *The Stirling numbers* $S(n,5)$ *satisfy*

$$\nu_2(S(8n,5)) = 1 \quad \textit{and} \quad \nu_2(S(8n+4,5)) \geq 2$$

and also

$$\nu_2(S(8n+3,5)) = 1 \quad \textit{and} \quad \nu_2(S(8n+7,5)) \geq 2.$$

Proof. The identity

$$24S(8n,5) = 5^{8n-1} - 4^{8n} + 2\cdot 3^{8n} - 2^{8n+1} + 1$$

is considered modulo 32. Using $5^8 \equiv 1$ and $5^7 \equiv 13$, it follows that $5^{8n-1} \equiv 13$. Also, $4^{8n} \equiv 0$ and $3^{8n} \equiv 1$. Therefore

$$5^{8n-1} - 4^{8n} + 2\cdot 3^{8n} - 2^{8n+1} + 1 \equiv 16 \bmod 32.$$

This gives $24S(8n,5) = 32t+16$ for some $t \in \mathbb{N}$ leading to $3S(8n,5) = 2(2t+1)$. Therefore $\nu_2 S(8n,5) = 1$.

The valuation of $S(8n+4,5)$ comes from the relation

$$24S(8n+4,5) = 5^{8n+3} - 4^{8n+4} + 2\cdot 3^{8n+4} - 2^{8n+5} + 1$$

modulo 32. Proceeding as before, it follows that $24S(8n+4,5) \equiv 0 \bmod 32$. Therefore $24S(8n+4,5) = 32t$ for some $t \in \mathbb{N}$. This yields $\nu_2(S(8n+4,5)) \geq 2$. The proof of the remaining cases is similar. □

Exercise 7.4.5. Give proofs of Theorems 7.4.1 and 7.4.2 in the style of the proof of Lemma 7.4.4.

Note 7.4.6. The results described in Lemmas 7.4.3 and 7.4.4 can be described in terms of a tree similar to the example in Note 1.7.3. The procedure described here generates the **valuation tree** associated to the p-adic valuation of a sequence $\{x_n : n \in \mathbb{N}\}$. Each of these trees has a **branching number** that depends on the prime p and the sequence $\{x_n\}$. The branching number is denoted by $\mathfrak{b} = \mathfrak{b}(p; x_n)$. For clarity, in the construction described next, the prime p and the branching number $\mathfrak{b}$ will be assumed to be equal to 2.

The construction of the tree begins with a **root vertex**. This vertex represents the whole set $\mathbb{N}$ and it forms the 0**th level** of the tree. Now assume that the kth level has been formed. This level represents *some* of the modular classes modulo 2^k. The transition to the next level is achieved by the following rules: let n_0 be the label of a vertex at the kth level. The label indicates that the vertex corresponds to the class

$$\mathfrak{a}_{n_0,k} = \{n \in \mathbb{N} : \, n \equiv n_0 \bmod 2^k\}.$$

Then the following question is asked:

Does the valuation $\{\nu_2(x_n) : \, n \in \mathfrak{a}_{n_0,k}\}$ *reduce to a single value?*

If the answer is yes, the vertex n_0 is declared to be a **terminal vertex** and the common value of the valuation is attached to n_0. If the answer is no, then the vertex n_0 is split into two classes modulo 2^{k+1}, namely,

$$\{n \in \mathbb{N} : \, n \equiv n_0 \bmod 2^{k+1}\} \quad \text{and} \quad \{n \in \mathbb{N} : \, n \equiv n_0 + 2^k \bmod 2^{k+1}\}.$$

The vertices produced by this splitting form the $(k+1)$st level.

This process is now applied to the sequence $x_n = S(n,5)$ and the prime $p = 2$. The valuation tree starts with a root vertex representing all $\mathbb{N}$. At this point, the question is whether $\{\nu_2(S(n,5)) : \, n \in \mathbb{N}\}$ is independent of n. The values $S(5,5) = 1$ and $S(7,5) = 140 = 2^2 \cdot 5 \cdot 7$ show that $\nu_2(S(5,5)) = 0$ and $\nu_2(S(7,5)) = 2$. Therefore the valuation $\nu_2(S(n,5))$ depends on n and the answer is no. This leads to a splitting of the root vertex into two vertices: one labeled 0, which represents the class $\mathfrak{a}_{0,1} = \{n \in \mathbb{N} : n \equiv 0 \bmod 2\}$, and the second one, labeled 1, representing the class $\mathfrak{a}_{1,1} = \{n \in \mathbb{N} : n \equiv 1 \bmod 2\}$. These two classes form the first level. The reader can check that each of these two classes do not have a constant 2-adic valuation and the process continues to the next level.

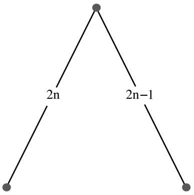


Figure 7.4.2. The first level of the tree for $S(n,5)$.

The class $\mathfrak{a}_{0,1}$ now splits into

$$\mathfrak{a}_{0,2} = \{n \in \mathbb{N} : n \equiv 0 \bmod 2^2\} \quad \text{and} \quad \mathfrak{a}_{2,2} = \{n \in \mathbb{N} : n \equiv 2 \bmod 2^2\}$$

and $\mathfrak{a}_{1,1}$ splits into

$$\mathfrak{a}_{1,2} = \{n \in \mathbb{N} : n \equiv 1 \bmod 2^2\} \quad \text{and} \quad \mathfrak{a}_{3,2} = \{n \in \mathbb{N} : n \equiv 3 \bmod 2^2\}.$$

The construction of the first two levels is depicted in Figure 7.4.3.

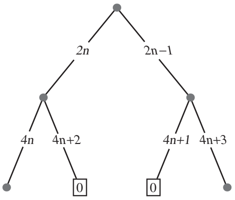


Figure 7.4.3. The first two levels of the tree for $S(n,5)$

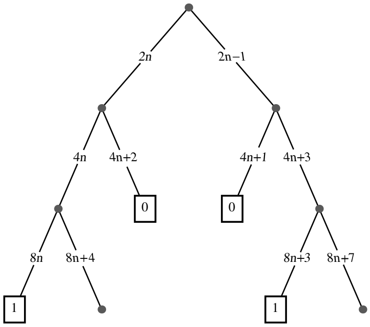


Figure 7.4.4. The first three levels of the tree for $S(n,5)$.

The vertices marked with $4n+1$ and $4n+2$ terminate at level 2. These correspond to the classes $\mathfrak{a}_{1,2}$ and $\mathfrak{a}_{2,2}$, respectively. They are both marked with 0, according to Lemma 7.4.3. The vertices marked $4n$ and $4n+3$, corresponding to the classes $\mathfrak{a}_{0,2}$ and $\mathfrak{a}_{3,2}$, respectively, are split to produce the vertices $8n$, $8n+4$ and $8n+3$, $8n+7$. These form the **third level**. Lemma 7.4.4 states that the vertices labeled

$8n$ and $8n+3$ terminate at this level and $8n+4$, $8n+7$ split into the four vertices $16n$, $16n+8$, $16n+7$, $16n+15$. These vertices form the **fourth level**.

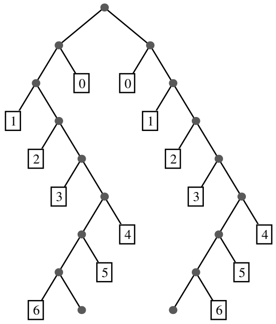


Figure 7.4.5. The continuation of the tree for $S(n,5)$.

The main result of T. Amdeberhan, D. Manna, and V. Moll [**10**] is stated next.

Theorem 7.4.7. *The valuation tree associated to the* 2*-adic valuation of* $S(n,5)$ *has, at every level starting with the third one, four vertices. At each level, two of these vertices terminate and the other two split to form the next level.*

Conjecture 7.4.8. *The same type of behavior occurs for the tree associated to* $S(n,k)$ *for* $k \geq 6$*. The corresponding tree begins as before, with a double splitting. At some point this process changes and half of the vertices terminate and the other half split. Eventually the number of vertices per level remains constant.*

Note 7.4.9. For k fixed, the sequence $\nu_2(S(n,k))$ offers a wide variety of profiles. The next sequence of figures offers a sample of them. It is unknown how to predict the form of the graph in terms of the fixed index k.

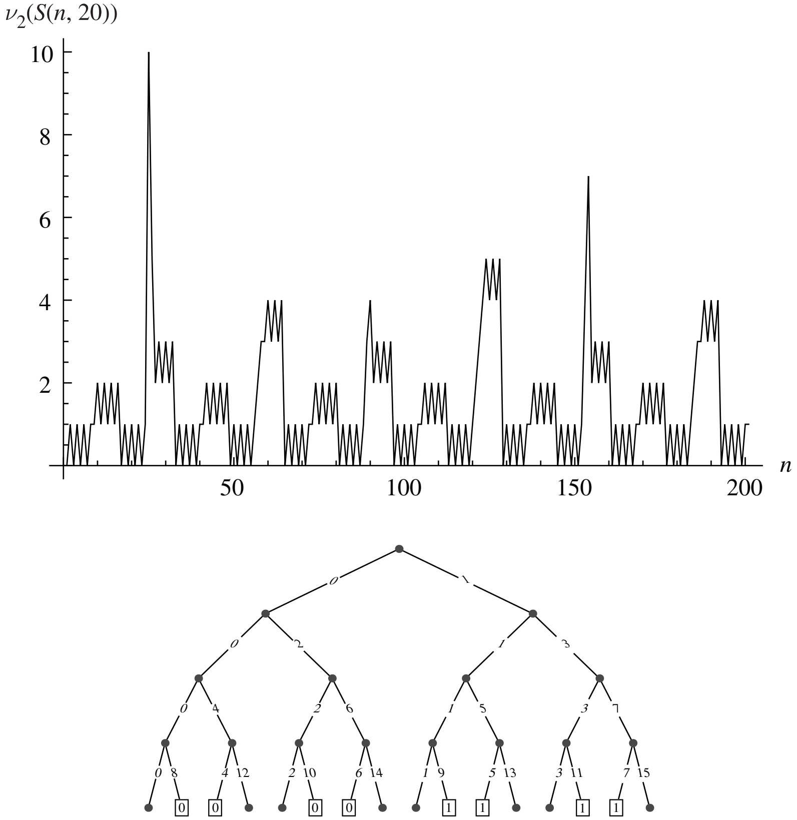
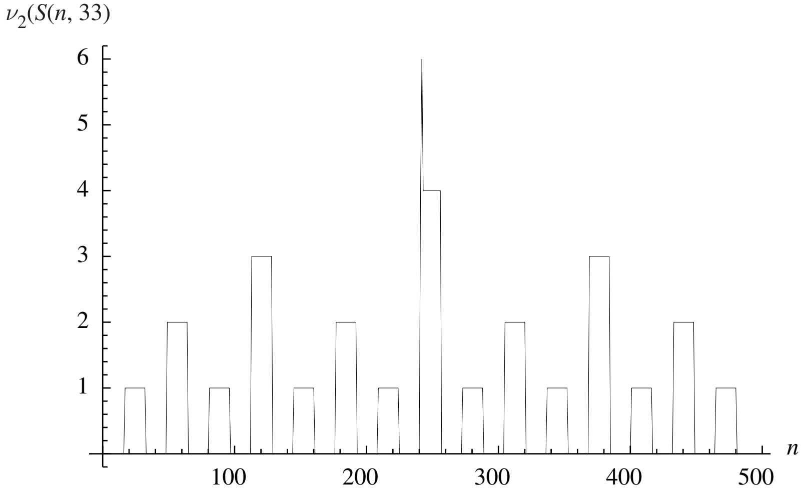


Figure 7.4.6. The 2-adic valuation of $S(n, 20)$.



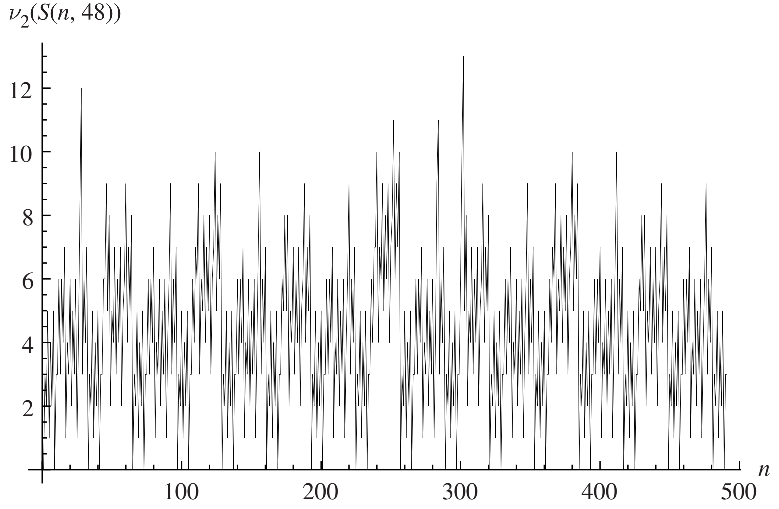


Figure 7.4.7. The 2-adic valuation of $S(n, 33)$ and $S(n, 48)$.

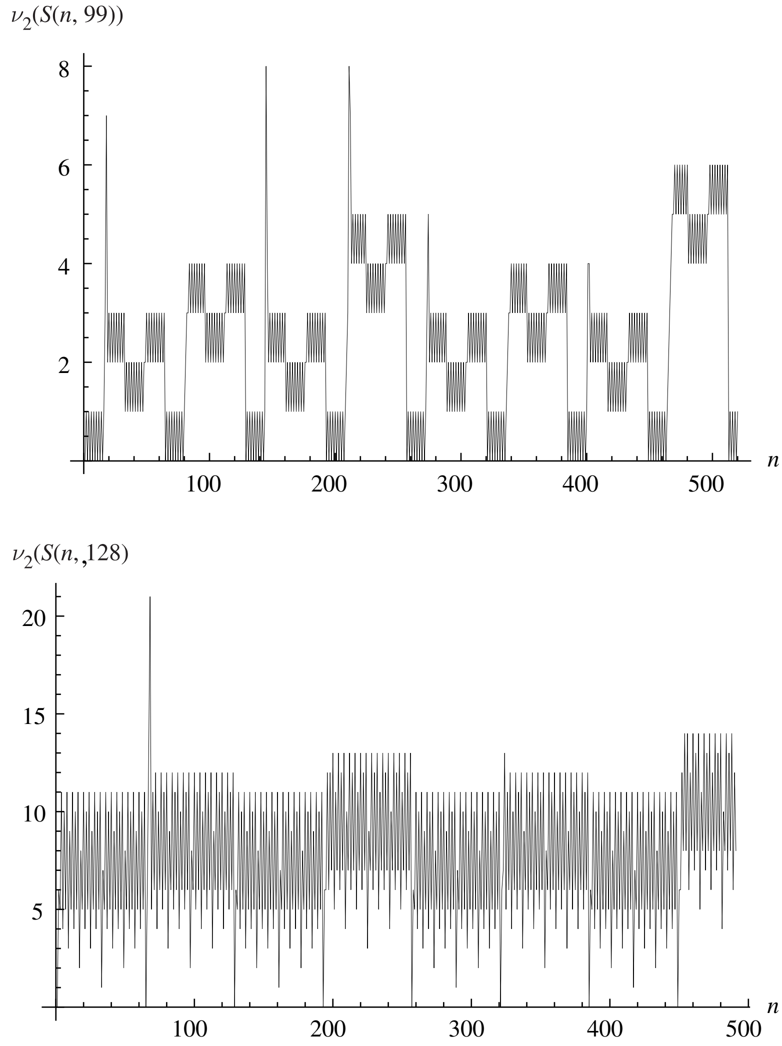


Figure 7.4.8. The 2-adic valuation of $S(n, 99)$ and $S(n, 128)$.

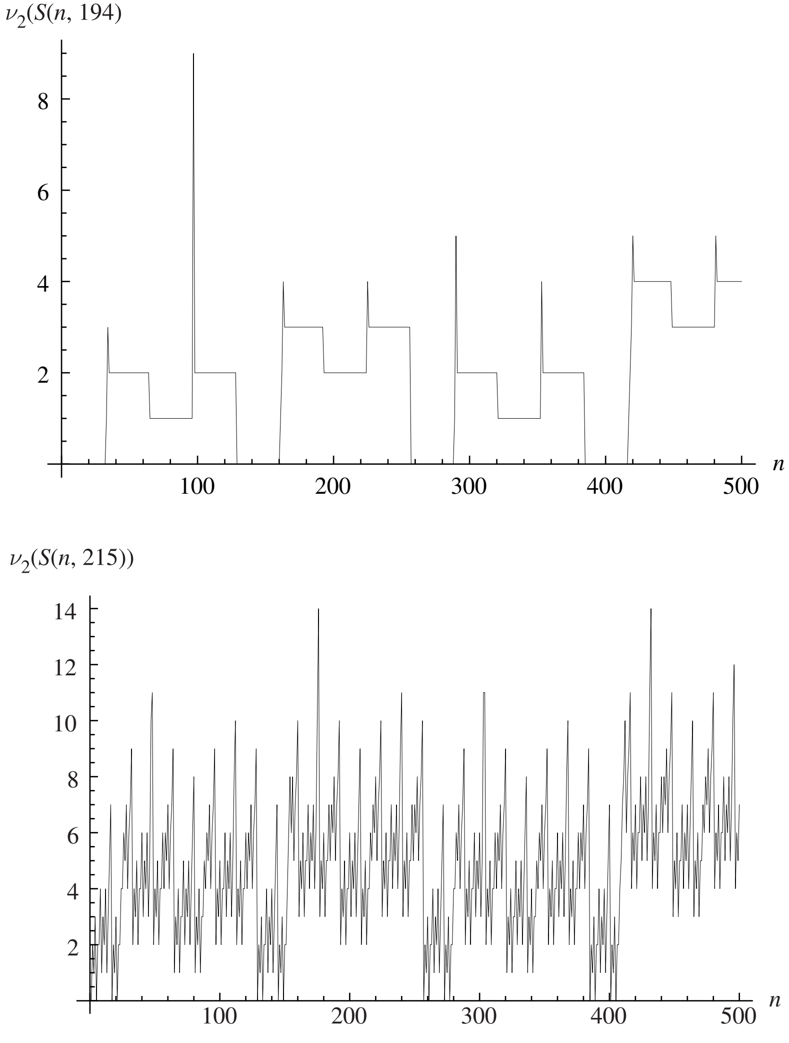


Figure 7.4.9. The 2-adic valuation of $S(n, 194)$ and $S(n, 215)$.

Note 7.4.10. There are many naturally occuring sequences whose p-adic valuations are capable of a complete analytic description. The case of the **ASM-numbers**, defined in (1.3.10) by

$$A_n = \prod_{j=0}^{n-1} \frac{(3j+1)!}{(n+j)!}, \tag{7.4.15}$$

has been described completely. Figure 7.4.10 shows the 2-adic valuation of A_n.

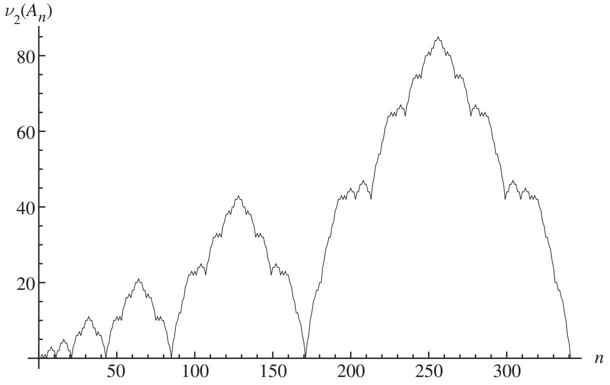


Figure 7.4.10. The 2-adic valuation of ASM-numbers.

The sequence A_n counts a famous class of matrices. An **alternating sign matrix** is an array of 0, 1, and -1 such that the entries of each row and column add up to 1 and the nonzero entries of a given row/column alternate. After a fascinating sequence of events, D. Zeilberger [**321**] proved that the numbers of such matrices is given by (7.4.15). In particular, the numbers A_n are integers—not an obvious fact.

The story behind this formula and its many combinatorial interpretations are given in D. Bressoud's book [**78**].

The first step in the analysis of $\nu_2(A_n)$ was to characterize the indices n for which A_n is odd. These are the values where the graph in Figure 7.4.10 achieves its minimum. This sequence of indices starts as

$$1,\ 3,\ 5,\ 11,\ 21,\ 43,\ 85,\ 171,\ 341,\ 683, \tag{7.4.16}$$

and by looking into **Sloane's Encyclopedia of Integer Sequences**, we see that they were recognized as the **Jacobsthal numbers**, with label $A001045$. These numbers satisfy the recurrence

$$J_n = J_{n-1} + 2J_{n-2}, \quad J_0 = 1,\; J_1 = 1.$$

The many interpretations of these numbers include the number of ways to tile a $3 \times (n-1)$ rectangle with squares of size 1 or 2 and also as the numerators in the reduced fraction

$$\frac{1}{2} - \frac{1}{4} + \frac{1}{8} - \frac{1}{16} + \frac{1}{32} - \cdots . \tag{7.4.17}$$

The complete description of the p-adic valuation of ASM-numbers can be found in the paper by E. Beyerstedt, V. Moll, and X. Sun [**53**] as well as in the paper by V. Moll and X. Sun [**286**].

The main result is an expression for $\nu_p(A_n)$ similar to the content of Exercise 2.6.3, where the classical series for the valuation $\nu_p(n)$ is expressed as a series in which each summand is a periodic function of period p^j.

Theorem 7.4.11. *Let $n \in \mathbb{N}$ and let $p \geq 5$ be a prime. Define*

$$\text{Per}_{j,p}(n) = \begin{cases} 0 & \textit{if } 0 \leq n \leq \left\lfloor \frac{p^j+1}{3} \right\rfloor, \\ n - \left\lfloor \frac{p^j+1}{3} \right\rfloor & \textit{if } \left\lfloor \frac{p^j+1}{3} \right\rfloor + 1 \leq n \leq \frac{p^j-1}{2}, \\ \left\lfloor \frac{2p^j+1}{3} \right\rfloor - n & \textit{if } \frac{p^j+1}{2} \leq n \leq \left\lfloor \frac{2p^j+1}{3} \right\rfloor, \\ 0 & \textit{if } \left\lfloor \frac{2p^j+1}{3} \right\rfloor + 1 \leq n \leq p^j - 1. \end{cases}$$

Then

$$\nu_p(A_n) = \sum_{j=1}^{\infty} \text{Per}_{j,p}\left(n \mod p^j\right).$$

Each summand in the series is of period p^j.

Note 7.4.12. The arithmetical statements about A_n can be extended to the sequence

$$A_n(q) := \prod_{j=0}^{n-1} \frac{(qj+1)!}{(n+j)!},$$

for $q \in \mathbb{N}$ with $q \geq 3$. The case of $q = 3$ corresponds to the ASM-numbers. An interesting question is to find a combinatorial interpretation of $A_n(q)$; that is, what do these numbers count?

Chapter 8

Rational Functions

8.1. Introduction

The first type of elements in the class of **elementary functions** is the **polynomials**, described in Chapter 4. This chapter considers a second fundamental class of elementary functions: the **rational functions**.

Definition 8.1.1. A **rational function** is the quotient of two polynomials, that is, an expression of the form

$$R(x) = \frac{A(x)}{B(x)} = \frac{a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0}{b_m x^m + b_{m-1} x^{m-1} + \cdots + b_1 x + b_0}. \tag{8.1.1}$$

The parameters a_i will be called the **numerator coefficients** of R and the b_i will be called the **denominator coefficients** of R. The collection

$$\{a_n,\, a_{n-1},\, \ldots, a_0; b_m,\, b_{m-1}, \ldots,\, b_0\}$$

is the **coefficients** of R.

In the form above, it may be assumed that the polynomials A and B are relatively prime; that is, common factors are canceled. As in the case of polynomials, the coefficients are taken from one of the number systems described in Chapter 1. This determines the name of the function. For instance the term a **real rational functions** refers to the situation when $a_i,\, b_j \in \mathbb{R}$.

Now assume that R is a complex rational function. Factoring the polynomials A and B over $\mathbb{C}$, the function R in (8.1.1) can be written in the form

$$R(x) = \frac{A(x)}{B(x)} = \frac{a_n(x-z_1)^{n_1}(x-z_2)^{n_2}\cdots(x-z_r)^{n_r}}{b_m(x-w_1)^{m_1}(x-w_2)^{m_2}\cdots(x-w_s)^{m_s}}. \tag{8.1.2}$$

Definition 8.1.2. The numbers z_j, where the numerator of R vanishes, are called the **zeros** of R and the integer n_j is the **multiplicity** of z_j. The numbers w_j, where the denominator of R vanishes, are called the **poles** of R and the numbers m_j are the multiplicity of w_j. A **simple pole** is a pole of mutiplicity 1.

Note 8.1.3. The factorization of the rational function (8.1.2) has a traditional normalization in the case of real coefficients. In this situation, the poles w_j come in complex conjugate pairs. Moreover, the multiplicity of w_j is the same as that of its conjugate. Then, if $w_j = u + iv$, the corresponding term is written as

$$(x-u-iv)(x-u+iv) = x^2 - 2ux + u^2 + v^2. \tag{8.1.3}$$

There are many interesting classes of rational functions throughout the literature. Two such examples are described next.

Example 8.1.4. A **bilinear transformation** is defined by

$$T(x) = \frac{ax+b}{cx+d}, \tag{8.1.4}$$

with a, b, c, $d \in \mathbb{C}$ and $ad - bc \neq 0$. This last condition implies that T is not constant. The function T maps $\mathbb{C} - \{-d/c\}$ to $\mathbb{C} - \{a/c\}$. It is natural to extend the definition of T to $\mathbb{C} \cup \{\infty\}$ via $T(-d/c) = \infty$ and $T(\infty) = a/c$.

Exercise 8.1.5. Check that the map T above has an inverse that is also bilinear. Prove that the composition of two of these maps produces one of the same type. The composition rule is given by matrix multiplication

$$\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} \times \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} = \begin{pmatrix} a_1a_2 + b_1c_2 & a_1b_2 + b_1d_2 \\ c_1a_2 + d_1c_2 & c_1b_2 + d_1d_2 \end{pmatrix}. \tag{8.1.5}$$

Therefore the set of all bilinear transformations forms a group, called the **group of Möbius transformations**. The reader will find more information in the book by A. Beardon [**44**].

Example 8.1.6. A second class of rational functions comes from trigonometry. This is the topic of Chapter 12. The addition theorem for trigonometric functions, given as Theorem 12.5.1, shows that

$$\cot(x+y) = \frac{\cot\, x \cot\, y - 1}{\cot\, x + \cot\, y}. \tag{8.1.6}$$

In particular,

$$\cot(2x) = \frac{\cot^2 x - 1}{2\, \cot\, x}. \tag{8.1.7}$$

Iterating this argument produces a sequence of rational functions R_m defined by

$$\cot(mx) = R_m(\cot x). \tag{8.1.8}$$

For example, (8.1.7) shows that $R_2(t) = \dfrac{t^2-1}{2t}$. These functions will play an important role in Chapter 15.

Exercise 8.1.7. Check that the rational functions R_m commute under composition; that is, $R_m \circ R_n = R_n \circ R_m$. This is a rare event. In fact, a theorem of S. Lattés [**196**] shows that the class of commuting rational functions can be completely characterized: they come from the addition theorem for **elliptic functions**. The functions R_m form a special limiting subclass. See the text by H. P. McKean and V. Moll [**213**] for details.

8.2. The method of partial fractions

This section discusses the familiar representation of a rational function R in terms of simpler components. This is the **method of partial fractions**. The function is written as

$$R(x) = \frac{A(x)}{B(x)} \tag{8.2.1}$$

and it will be assumed first that the poles of R are simple. The function is written as

$$R(x) = \frac{A(x)}{(x-w_1)(x-w_2)\cdots(x-w_r)} \tag{8.2.2}$$

with w_j distinct. The poles of R are treated as parameters.

Definition 8.2.1. A rational function R is called **reduced** if it is written as $R(x) = A(x)/B(x)$ with $\gcd(A, B) = 1$ and $\deg(A) < \deg(B)$.

Exercise 8.2.2. The restriction $\deg(A) < \deg(B)$ may always be imposed. Otherwise divide A by B to produce

$$R(x) = P(x) + \frac{A_1(x)}{B(x)},$$

where P is a polynomial and $\deg(A_1) < \deg(B)$ is satisfied. Check the details.

Theorem 8.2.3. *Assume R is a reduced rational function with simple poles w_j. Then there are constants α_j such that*

$$R(x) = \sum_{j=1}^{r} \frac{\alpha_j}{x - w_j}. \tag{8.2.3}$$

The value of α_j is given by

$$\alpha_j = \frac{A(w_j)}{B'(w_j)}. \tag{8.2.4}$$

Proof. Assume that such a decomposition exists. Then

$$\frac{A(x)(x - w_j)}{B(x)} = \sum_{k \neq j} \frac{\alpha_k (x - w_j)}{x - w_k} + \alpha_j. \tag{8.2.5}$$

Let $x \to w_j$ to obtain the result. The proof of the existence of such a decomposition is left as the next exercise. □

Exercise 8.2.4. This is an alternative proof of Theorem 8.2.3. Write $B(x) = \prod_{j=1}^{r} (x - w_j)$ and check that $B'(w_k) = \prod_{j \neq k} (w_k - w_j)$. Construct the polynomial

$$F(x) = \sum_{i=1}^{r} \frac{A(w_i)}{B'(w_i)} \prod_{j \neq i} (x - w_j).$$

Prove that $F(x) = A(x)$. **Hint:** Verify that $F(w_k) = A(w_k)$ for $1 \leq k \leq r$ and $r = \deg(B) > \deg(A)$.

Exercise 8.2.5. Prove the existence of the decomposition. **Hint:** Write down a linear system for the unknowns α_j and evaluate its determinant. An alternative proof is by induction on the number of poles. **Hint:** Use the identity

$$\frac{1}{(x-w_1)(x-w_2)} = \frac{1}{(w_1-w_2)}\left[\frac{1}{x-w_1} - \frac{1}{x-w_2}\right].$$

The expressions become more elaborate if the rational function has poles of higher order. The simplest situation is described in the next exercise.

Exercise 8.2.6. Suppose $R(x)$ has a double pole at $x = w_1$. Combine the terms corresponding to $x = w_1$ and $x = w_1 + \varepsilon$, with $\varepsilon \to 0$ to conclude that R has an expansion of the form

$$R(x) = \frac{A(x)}{B(x)} = \frac{\alpha}{(x-w_1)^2} + \frac{\beta}{x-w_1} + H(x), \tag{8.2.6}$$

where $H(z)$ does not have a pole at $x = w_1$. Introduce the polynomial C by the relation $B(x) = (x-w_1)^2 C(x)$. Prove that

$$\alpha = \frac{A(w_1)}{C(w_1)} \tag{8.2.7}$$

and

$$\beta = \frac{A'(w_1)C(w_1) - A(w_1)C'(w_1)}{C(w_1)^2}. \tag{8.2.8}$$

Exercise 8.2.7. Let $P(x)$ be a polynomial and let $x = a$ be one of its roots. Prove that $x = a$ is a root of multiplicity higher than 1 if and only if $x = a$ is also a root of the derivative $P'(x)$.

Exercise 8.2.8. The method of partial fractions converts a reduced rational function $R(x)$ into a sum of simpler terms. Prove that R can be written in the form

$$\frac{A(x)}{B(x)} = \sum_{j=1}^{n}\sum_{k=1}^{c_j} \frac{A_{j,k}}{(x-w_j)^k} + \sum_{j=1}^{m}\sum_{k=1}^{d_j} \frac{B_{j,k}x + C_{j,k}}{(x^2+2u_jx+u_j^2+v_j^2)^k}. \tag{8.2.9}$$

The parameters w_j are the real poles of R and c_j the corresponding multiplicities. The complex roots appear in pairs $u_j \pm iv_j$ and have multiplicity d_j.

Note 8.2.9. The `Mathematica` command `Apart` gives the partial fraction decomposition of a rational function.

Note 8.2.10. The main goal of the method of partial fractions is to facilitate the integration of a rational function. This is discussed in Section 8.7. Preliminary details are given here.

In order to analyze the integral of R over $[0, \infty)$, separate the roots with multiplicity $d_j = 1$ and write

$$B_j x + C_j = \frac{1}{2} B_j (2x + 2u_j) + C_j - u_j B_j := E_j (2x + 2u_j) + F_j,$$

to replace (8.2.9) by

$$\begin{aligned} \frac{A(x)}{B(x)} \quad = \quad & \sum_{j=1}^{n} \frac{A_{j,1}}{x - w_j} + \sum_{j=1}^{n} \sum_{k=2}^{c_j > 1} \frac{A_{j,k}}{(x - w_j)^k} \\ & + \sum_{k=1}^{m} \frac{E_j(2x + 2u_j)}{x^2 + 2u_j x + u_j^2 + v_j^2} + \sum_{j=1}^{m} \frac{F_j}{x^2 + 2u_j x + u_j^2 + u_j^2} \\ & + \sum_{j=1}^{m} \sum_{k=2}^{d_j > 1} \frac{E_j(2x + 2u_j)}{(x^2 + 2u_j x + u_j^2 + v_j^2)^k} \\ & + \sum_{j=1}^{m} \sum_{k=2}^{d_j > 1} \frac{F_j}{(x^2 + 2u_j x + v_j^2 + v_j^2)^k}. \end{aligned}$$

Exercise 8.2.11. A very clever method to obtain the partial fraction decomposition of a rational function appeared in the paper by M. Hirschhorn [**170**]. This exercise outlines the procedure.

Step 1. Suppose $u + v = 1$. Prove by induction that

$$\frac{1}{uv^n} = \frac{1}{u} + \frac{1}{v^n} + \frac{1}{v^{n-1}} + \cdots + \frac{1}{v}.$$

Step 2. Use the result of Step 1 and prove by induction that if $u + v = 1$, then

$$\frac{1}{u^m v^n} = \sum_{k=0}^{m-1} \frac{\binom{n-1+k}{k}}{u^{m-k}} + \sum_{j=0}^{n-1} \frac{\binom{m-1+j}{j}}{v^{n-j}}.$$

Step 3. Apply the result of Step 2 to u/c and v/c to produce an identity under the condition $u + v = c$. Replace v by $-v$ and impose the condition $u - v = c$. Finally let $u = x - a$ and $v = x - b$ to obtain

$$\begin{aligned}\frac{1}{(x-a)^m\,(x-b)^n} &= (-1)^n \sum_{k=0}^{m-1} \frac{(b-a)^{-n-k}\binom{n-1+k}{k}}{(x-a)^{m-k}} \\ &\quad + (-1)^m \sum_{j=0}^{n-1} \frac{(a-b)^{-m-j}\binom{m-1+j}{j}}{(x-b)^{n-j}}.\end{aligned}$$

Step 4. Use the result recursively to produce the partial fraction expansion of

$$R(x) = \frac{1}{(x-1)^4(x-2)^3(x-3)^2}.$$

8.3. Rational generating functions

Rational functions appear as the generating function of some interesting sequences. For example, the Fibonacci numbers F_n considered in Chapter 3 have a rational generating function:

$$\sum_{n=0}^{\infty} F_n x^n = \frac{x}{1-x-x^2}. \tag{8.3.1}$$

This example illustrates a general result. The statement employs the notion of reduced rational function given in Definition 8.2.1.

Theorem 8.3.1. *Let $\{a_n\}$ be a sequence of real numbers and let*

$$R(x) = \sum_{n=0}^{\infty} a_n x^n$$

be its generating function. Then a_n satisfies a linear recurrence with constant coefficients if and only if $R(x)$ is a reduced rational function.

Proof. Assume the coefficients $\{a_n\}$ satisfy the recurrence

$$a_n = \sum_{j=1}^{k} t_j a_{n-j}. \tag{8.3.2}$$

Multiply this relation by x^n and sum from $n = k$ to infinity. This produces

$$\begin{aligned}\sum_{n=k}^{\infty} a_n x^n &= \sum_{n=k}^{\infty}\left(\sum_{j=1}^{k} t_j a_{n-j}\right) x^n \\ &= \sum_{j=1}^{k} t_j x^j \left(\sum_{n=k}^{\infty} a_{n-j} x^{n-j}\right) \\ &= R(x)\sum_{j=1}^{k} t_j x^j - \sum_{j=1}^{k-1} t_j x^j \sum_{n=0}^{k-j-1} a_n x^n.\end{aligned}$$

Define $t_0 = -1$ and use

$$\sum_{n=k}^{\infty} a_n x^n = R(x) - \sum_{n=0}^{k-1} a_n x^n$$

to produce

$$\left(\sum_{j=0}^{k} t_k x^j\right) R(x) = -\sum_{j=0}^{k-1} t_j x^j \left(\sum_{n=0}^{k-j-1} a_n x^n\right). \tag{8.3.3}$$

This shows that $R(x)$ is a reduced rational function. Moreover, its denominator is

$$B(x) = t_0 + t_1 x + t_2 x^2 + \cdots + t_k x^k \tag{8.3.4}$$

and its degree is at most the order of the recurrence satisfied by $\{a_n\}$. Observe that the denominator $B(x)$ can be read directly from the recurrence (8.3.2).

To establish the converse, write $R(x) = A(x)/B(x)$ with B as in (8.3.4). Assume first that $B(0) \neq 0$ and that the roots w_j of B are distinct. The partial fraction decomposition of R can be written as

$$\begin{aligned} R(x) &= \sum_{j=1}^{k} \frac{\alpha_j}{x - w_j} \\ &= -\sum_{j=1}^{k} \frac{\alpha_j}{w_j} \cdot \frac{1}{1 - \frac{x}{w_j}} \\ &= -\sum_{n=0}^{\infty} \sum_{j=1}^{k} \frac{\alpha_j}{w_j^{n+1}} x^n. \end{aligned}$$

Therefore

$$R(x) = \sum_{n=0}^{\infty} a_n x^n \tag{8.3.5}$$

with

$$a_n = -\sum_{j=1}^{k} \frac{\alpha_j}{w_j^{n+1}}. \tag{8.3.6}$$

The root w_j satisfies

$$B(w_j) = t_0 + t_1 w_j + t_2 w_j^2 + \cdots + t_k w_j^k = 0. \tag{8.3.7}$$

This gives

$$\begin{aligned} \sum_{s=0}^{k} t_s a_{n-s} &= -\sum_{s=0}^{k} t_s \sum_{j=1}^{k} \frac{\alpha_j}{w_j^{n+1}} w_j^s \\ &= -\sum_{j=1}^{k} \left(\sum_{s=0}^{k} t_s w_j^s \right) \frac{\alpha_j}{w_j^{n+1}} \\ &\equiv 0. \end{aligned}$$

This is the recurrence for $\{a_n\}$. □

Exercise 8.3.2. Complete the proof for the case of repeated roots. **Hint:** The coefficients are continuous functions of the roots.

8.4. The operator point of view

The following exercise can be carried out in elementary terms: find a recurrence for the sequence of even Fibonacci numbers $\{F_{2n} : n \in \mathbb{N}\}$.

The existence of such a recurrence can be solved directly for any sequence $\{a_n\}$ with rational generating function. Indeed, if

$$R(x) = \sum_{n=0}^{\infty} a_n x^n, \tag{8.4.1}$$

then

$$\sum_{n=0}^{\infty} a_{2n} x^n = \frac{R(\sqrt{x}) + R(-\sqrt{x})}{2}, \tag{8.4.2}$$

and the reader can check that the right-hand side of (8.4.2) is also a rational function of x. The result now follows from Theorem 8.3.1.

A simple procedure to actually find the recurrence is outlined next. The proof of Theorem 8.3.1 shows that the recurrence satisfied by $\{a_n\}$ is

$$\sum_{j=0}^{k} t_j a_{n-j} = 0, \tag{8.4.3}$$

and replacing n by $n+k$, it becomes

$$\sum_{j=0}^{k} t_j a_{n+k-j} = 0. \tag{8.4.4}$$

Introduce the operator S acting on sequences by

$$S \cdot \{a_n\} = \{a_{n+1}\}. \tag{8.4.5}$$

Then (8.4.4) can be written as

$$\sum_{j=0}^{k} t_j S^{k-j} \cdot \{a_n\} = 0, \tag{8.4.6}$$

where the power S^j represents S composed with itself j times.

In order to write this equation in operator form, define

$$B_1(x) = x^k B(x^{-1}) \tag{8.4.7}$$

where B is the denominator of the rational function R. This is given by

$$B(x) = t_0 + t_1 x + t_2 x^2 + \cdots + t_k x^k. \tag{8.4.8}$$

Then (8.4.6) can be written as

$$B_1(S) \cdot \{a_n\} = 0. \tag{8.4.9}$$

This representation is now employed to produce a recurrence for $\{a_{2n}\}$. The task at hand is to produce a polynomial in S^2 that annihilates this sequence. The natural idea is to multiply (8.4.9) by $B_1(-S)$ to obtain

$$B_1(-S) \cdot B_1(S) \cdot \{a_n\} = 0. \tag{8.4.10}$$

It turns out that the operator $B_1(-S) \cdot B_1(S)$ depends only on S^2. This yields the recurrence for $\{a_{2n}\}$. The next example illustrates the argument.

Example 8.4.1. The Fibonacci numbers F_n satisfy $F_{n+2} = F_{n+1} + F_n$. Then $B(x) = -x^2 + x + 1$ and $B_1(x) = x^2 + x - 1$. To produce a polynomial in x^2, compute

$$B_1(x) \cdot B_1(-x) = x^4 - 3x^2 + 1. \tag{8.4.11}$$

This yields $F_{n+4} - 3F_{n+2} + F_n = 0$. Now replace n by $2n$ to obtain the desired recurrence for the even Fibonacci numbers $X_n = F_{2n}$:

$$X_{n+2} - 3X_{n+1} + X_n = 0. \tag{8.4.12}$$

In operator form, this is $S^2 - 3S + 1 = B_1(\sqrt{S}) \cdot B_1(-\sqrt{S})$.

Exercise 8.4.2. Find a recurrence for $\{F_{2n+1} : n \in \mathbb{N}\}$ and for $\{F_{3n} : n \in \mathbb{N}\}$.

8.5. A dynamical system

In the process of developing a new procedure for the integration of rational functions, the author obtained a transformation on the coefficients of the integrand that preserves the value of the integral. The starting point was the attempt to evaluate the integral

$$I = \int_0^\infty R(x)\, dx$$

without computing the poles of R.

It turns out that the algorithm, explained in Chapter 15, only works for even rational functions. The decomposition

$$R(x) = \frac{1}{2}(R(x)+R(-x)) + \frac{1}{2}(R(x)-R(-x)) \equiv R_e(x) + R_o(x)$$

into the even and odd parts reduces the problem to the integration of the odd part. The change of variables $x \mapsto \sqrt{x}$ yields

$$\int_0^\infty R(x)\,dx = \int_0^\infty R_e(x)\,dx + \frac{1}{2}\int_0^\infty \mathfrak{F}(R(x))\,dx, \tag{8.5.1}$$

with

$$\mathfrak{F}(R(x)) = \frac{R(\sqrt{x}) - R(-\sqrt{x})}{2\sqrt{x}}. \tag{8.5.2}$$

Compare with (8.4.2).

Exercise 8.5.1. Prove that $\mathfrak{F}(R(x))$ is also a rational function.

Exercise 8.5.2. It is totally unclear that this procedure is an effective method to integrate. Check that (8.5.1) yields

$$\int_0^\infty \frac{dx}{x^2+x+3} = \int_0^\infty \frac{x^2+3}{x^4+5x^2+9}\,dx - \frac{1}{2}\int_0^\infty \frac{dx}{x^2+5x+9}.$$

The right-hand side seems more complicated than the original question.

In spite of its apparent failure to help in the question of integration, the map $\mathfrak{F}$ as a map on the space of rational functions, has many interesting properties. Some of them are described next. Details about this map appear in the papers by C. Bennett and E. Mosteig [**47**] and by G. Boros, M. Joyce, and V. Moll [**59**], in the multi-authored paper by G. Boros et al. [**60**], and in the work of E. Mosteig [**226**].

The definition of $\mathfrak{F}$ in terms of power series is given next. Let $R(x) = A(x)/B(x)$ be a rational function with expansion around $x=0$ of the form

$$R(x) = \sum_{k \gg -\infty}^{\infty} a_k x^k. \tag{8.5.3}$$

The notation indicates that, for some $N \in \mathbb{Z}$, the coefficients a_n vanish for $n < N$.

Exercise 8.5.3. Check that $\mathfrak{F}(R)$ has the expansion

$$\mathfrak{F}(R)(x) = \sum_{k \gg -\infty}^{\infty} a_{2k+1} x^k. \tag{8.5.4}$$

Definition 8.5.4. Let R be a rational function. The **orbit** of R under $\mathfrak{F}$ is the set of iterates

$$\mathrm{Orb}(R) = \{\mathfrak{F}^j(R) : j \in \mathbb{N}_0\}. \tag{8.5.5}$$

Powers of $\mathfrak{F}$ indicate composition.

Exercise 8.5.5. The orbit of an even function is simply $\{R, 0\}$.

8.5.1. Some fixed points of $\mathfrak{F}$. The simplest orbits are provided by functions fixed by $\mathfrak{F}$. Then the orbit reduces to a single element. These functions were classified in [**60**]. The exercises outline some of their properties.

Exercise 8.5.6. Let $R(x) = \sum\limits_{k=-N}^{\infty} a_k x^k$. Prove that

$$\mathfrak{F}(R)(x) = \sum_{k=-\lfloor (N+1)/2 \rfloor}^{\infty} a_{2k+1} x^k.$$

Exercise 8.5.7. Let R be a fixed point of $\mathfrak{F}$. Then the order of the pole at $x = 0$ is at most 1. **Hint:** Match the lowest-order terms.

Example 8.5.8. The function $R(x) = 1/x$ is a fixed point. It is also possible to have a fixed point without poles at $x = 0$ as the example $R(x) = 1/(1-x)$ shows.

Exercise 8.5.9. Let R be a fixed point of $\mathfrak{F}$ and let $m \in \mathbb{N}$ be odd. Then $\mathfrak{B}_m(R(x)) = x^{m-1}R(x^m)$ is also fixed by $\mathfrak{F}$.

Exercise 8.5.10. Exercise 8.5.9 applied to $R(x) = 1/(x-1)$ shows that, for m odd,

$$R_m(x) = \frac{x^{m-1}}{x^m - 1} \tag{8.5.6}$$

is a fixed point of $\mathfrak{F}$. Check this directly.

Note 8.5.11. The description of all the fixed points of $\mathfrak{F}$ requires the notion of **cyclotomic cosets**: given n, $r \in \mathbb{N}$ with r odd and $0 \leq n \leq r-1$, the set

$$C_{r,n} = \{2^s n \mod r : \ s \in \mathbb{Z}\}$$

is the 2-cyclotomic coset of n mod r. Observe that $C_{r,n}$ is a finite set. With λ a fixed primitive rth root of unity, define

$$f_{r,n}(x) = \sum_{m \in C_{r,n}} \frac{\lambda^m}{1 - \lambda^m x}.$$

The next theorem classifies all the fixed points of $\mathfrak{F}$. The details appear in [**60**].

Theorem 8.5.12. *A rational function is fixed by $\mathfrak{F}$ if and only if it is a linear combination of $1/x$ and the functions $f_{r,n}(x)$ for r odd and $0 \leq n \leq r-1$.*

8.5.2. A special subclass.

The function

$$R_{j,m}(x) = \frac{x^j}{x^m - 1} \quad \text{for } m \text{ odd and } j \in \mathbb{Z} \tag{8.5.7}$$

has interesting dynamic properties under the transformation $\mathfrak{F}$.

Exercise 8.5.13. Prove that

$$\mathfrak{F}\left(\frac{x^j}{x^m - 1} \right) = \frac{x^{\alpha_m(j)}}{x^m - 1},$$

where $\alpha_m(j) = m \left\lfloor \frac{j}{2} \right\rfloor - \frac{1}{2}(m-1)(j-1)$.

Thus the dynamical properties of the iterates $\mathfrak{F}^k(R)$ are reduced to those of α_m.

Note 8.5.14. The map α_m has interesting dynamical properties. A summary is presented here. Details appear in [**59**].

- The only fixed points of α_m are $j = -1$ and $j = m-1$.

- The iterates of α_m always reach the set $\{0, 1, 2, \ldots, m-2\}$ in a finite number of steps. Moreover this set is invariant under the action of α_m.

- Let $r \in \mathbb{N}$ and define $m = 2^r - 1$. The orbit of $1/(x^m - 1)$ has length r. Thus there are orbits of any given length. Compute the orbit starting at 0 and that starting at 2 to conclude that there are at least two orbits of length r.

- The integer m is a **pseudoprime** of base a if $a^{m-1} \equiv 1 \bmod m$. The relation to the problem discussed here is that if α_m has a unique orbit, then m is a pseudoprime of base 2.

- Let m be a prime. Recall that a is a **primitive root** of m if the powers $a^j \bmod m$ give all the nonzero residues modulo m. Suppose m is prime. Then α_m has a single orbit if and only if 2 is a primitive root modulo m. The primes $m \leq 100$ for which 2 is a primitive root are $\{3, 5, 11, 13, 19, 29, 37, 53, 59, 61, 67, 83\}$. E. Artin [**30**] conjectured that this occurs for infinitely many primes. The paper by M. R. Murty [**229**] contains information on this conjecture.

- Suppose m is a **Sophie Germain prime**, that is, a prime of the form $m = 2q + 1$ with q prime. Then there are at most two orbits. In the case of two orbits, both have the same length.

- Suppose α_m has an orbit of length n and $M_n := 2^n - 1$ is a Mersenne prime. Then m is an odd multiple of M_n.

8.6. Sums of four squares

Sums of squares played an important role in the early history of number theory. For example, Fermat proved that every prime $p \equiv 1 \bmod 4$ can be written as a sum of two squares. The beautiful proof by D. Zagier has been described in Chapter 1 as Theorem 1.7.12. Lagrange proved that every positive integer is a sum of four squares and Jacobi proved an expression for the number of such representations. These are gems of the past. This section presents a modern style proof of Lagrange's result. It appeared in the paper by G. E. Andrews, Shalosh B. Ekhad, and D. Zeilberger [**21**] and the two human authors have been in the past on opposite sides on the concept of a proof. See the paper by D. Zeilberger [**320**] and the response in the paper by G. E. Andrews [**20**]. The reader should be careful with making the wrong conclusions after reading these two papers. Reading the work by G. E. Andrews and P. Paule [**19**] and many other joint papers of these two authors should be included in the analysis of the so-called dispute between traditional methods of proof and the development of automatic ones.

The proof employs the rational function, defined for $n \in \mathbb{N}$, as

$$Y_n = Y_n(q) = \frac{1+q}{1-q} \cdot \frac{1+q^2}{1-q^2} \cdots \frac{1+q^n}{1-q^n}; \tag{8.6.1}$$

the natural extensions $Y_0 = 1$ and $Y_n = 0$ for $n < 0$ are adopted. Two identities are established first.

Lemma 8.6.1. *For $n \in \mathbb{N}$,*

$$\sum_{k=-n}^{n} \frac{4(-q)^k}{(1+q^k)^2} Y_n^2 Y_{n+k} Y_{n-k} = 1, \tag{8.6.2}$$

and

$$\sum_{k=0}^{n} \frac{2(-q^{n+1})^k}{1+q^k} \frac{Y_k}{Y_n} = \sum_{k=-n}^{n} (-q)^{k^2}. \tag{8.6.3}$$

Proof. Let $F_1(n,k;q)$ be the summand in (8.6.2) and let $H_1(n;q)$ denote the sum of $F_1(n,k;q)$ for all $k \in \mathbb{Z}$. Observe that $F_1(n,k;q)$ vanishes if $k > n$ or $k < -n$, so the sum is actually finite. The proof is based on the construction of a function $R_1(n,k,q)$, rational in q, such that

$$G_1(n,k;q) := R_1(n,k;q) F_1(n,k;q) \tag{8.6.4}$$

satisfies the relation

$$F_1(n+1,k;q) - F_1(n,k;q) = G_1(n,k;q) - G_1(n,k-1;q). \tag{8.6.5}$$

This can be done completely automatically using the q-Zeilberger algorithm developed in the paper by P. Paule and A. Riese [**244**] and implemented in C. Koutschan's package `HolonomicFunctions`. The output is

$$R_1(n,k;q) = \frac{q^{n-k+1}(1+q^{2n+2})(1+q^k)^2(1+q^{n+k+1})}{(1-q^{n+1})^3(1-q^{n+k+1})(1+q^{n+1})}. \tag{8.6.6}$$

For $k > n$ or $k < -n$ the expression $G_1(n,k;q)$ vanishes, since F_1 does.

Exercise 8.6.2. Check (8.6.5).

The last step in the proof is to define

$$H_1(n;q) = \sum_k F_1(n,k;q)$$

and to sum (8.6.5) over all $k \in \mathbb{Z}$ to produce

$$H_1(n+1;q) = H_1(n;q). \tag{8.6.7}$$

The value $H_1(0;q) = 1$ proves the identity (8.6.2). The proof of (8.6.3) is outlined in the next exercise. □

Exercise 8.6.3. With notation similar to that in the proof, use the q-Zeilberger algorithm to find the rational function

$$R_2(n,k;q) = \frac{(-q)^{n+1}(1+q^k)}{1+q^{n+1}}, \tag{8.6.8}$$

which gives the recurrence $H_2(n+1;q) - H_2(n;q) = 2(-q)^{(n+1)^2}$ and establishes (8.6.3).

A classical identity of Jacobi is given as the next exercise.

Exercise 8.6.4. Divide (8.6.2) by Y_n^4 and let $n \to \infty$ in (8.6.2) and (8.6.3) to obtain

$$\left(\sum_{k=-\infty}^{\infty} q^{k^2} \right)^4 = 1 + 8 \sum_{k=1}^{\infty} \frac{q^k}{(1+(-q)^k)^2}. \tag{8.6.9}$$

These preliminary results provide a proof of Jacobi's theorem. Define $r_4(n)$ as the number of ordered quadruples $(x_1,x_2,x_3,x_4) \in \mathbb{Z}^4$ that satisfy $x_1^2 + x_2^2 + x_3^2 + x_4^2 = n$.

Theorem 8.6.5. *The number of ways $r_4(n)$ to write a number n as a sum of four squares is given by* 8 *times the sum of the divisors of n that are not multiples of* 4. *The number* 1 *is always part of the sum, so every positive integer is the sum of four squares.*

Proof. The coefficient of q^n in the expansion of the fourth power on the left-hand side of (8.6.9) is $r_4(n)$. To expand the right-hand side, use

$$\frac{z}{(1+z)^2} = \sum_{j=1}^{\infty} (-1)^{j+1} j z^j \tag{8.6.10}$$

with $z = (-q)^k$ to write the right-hand side as

$$\sum_{k=1}^{\infty} \sum_{j=1}^{\infty} (-1)^{(k+1)(j+1)} j q^{jk} = \sum_{n=1}^{\infty} q^n \left(\sum_{j|n} (-1)^{(j+1)(n/j+1)} j \right).$$

The coefficient of j is -1 if both j and n/j are even; otherwise it is $+1$. Therefore $r_4(n)$ is the sum of the divisors of n that are not divisible by 4. □

Comments on the proof.

(1) The identity (8.6.2) produces an interesting cancelation of the singularities on the left-hand side to produce the constant 1. Observe that

$$\lim_{q \to 1} (1-q)^n Y_n(q) := c_n = \frac{2^n}{n!} \tag{8.6.11}$$

so $Y_n(q) \sim c_n/(1-q)^n$ as $q \to 1$.

(2) The sum on the right-hand side of (8.6.3) is the finite version of Jacobi's theta function. The reader will find information about these functions in the text **Elliptic Curves** [**213**].

(3) The proofs of the identities appearing in (8.6.2) and (8.6.3) can now be obtained in completely automatic form. Naturally it is possible to completely hide the computer from the proof and to state the proof in the following terms:

Computer-free proof of Lemma 8.6.1. Define

$$Y_n = Y_n(q) = \frac{1+q}{1-q} \cdot \frac{1+q^2}{1-q^2} \cdots \frac{1+q^n}{1-q^n}$$

for $n \in \mathbb{N}$ with $Y_0 = 1$ and $Y_n = 0$ for $n < 0$. Introduce

$$F_1(n,k;q) = \frac{4(-q)^k}{(1+q^k)^2} Y_n^2 Y_{n+k} Y_{n-k}$$

and let

$$T_1(n;q) = \sum_{k=-n}^{n} F_1(n,k;q).$$

Define $G_1(n,k;q)$ by $R_1(n,k;q)F_1(n,k;q)$ with

$$R_1(n,k;q) = \frac{q^{n-k+1}(1+q^{2n+2})(1+q^k)^2(1+q^{n+k+1})}{(1-q^{n+1})^3(1-q^{n+k+1})(1+q^{n+1})}.$$

Then

$$F_1(n+1,k;q) - F_1(n,k;q) = G_1(n,k;q) - G_1(n,k-1;q)$$

holds. Sum this recurrence for all values of $k \in \mathbb{Z}$ to obtain

$$T_1(n+1;q) = T_1(n,q).$$

The initial value $T_1(0;q) = 1$ gives the result.

***This is a completely correct but totally dishonest proof*.**

8.7. The integration of rational functions

The problem of integration of rational functions $R(x) = A(x)/B(x)$ was considered by J. Bernoulli in the eighteenth century. He completed Leibniz's original attempt at a general partial fraction decomposition of $R(x)$. The main difficulty associated with this procedure is to obtain a complete factorization of $B(x)$ over $\mathbb{R}$. It is known that a primitive of a rational function is always elementary: it consists of a new rational function (its rational part) and the logarithm of a second rational function (its transcendental part). These logarithms include complex arguments as in the case of $R(x) = 1/(x^2+1)$. In his classic monograph [**158**], G. H. Hardy states: *The solution of the problem (of definite integration) in the case of a rational function may therefore be said to be complete; for the difficulty with regard to the explicit solution of algebraic equations is one not of inadequate knowledge but of proved impossibility.* He goes on to add: *It appears from the preceding paragraphs that we can always find the rational part of the integral, and can find the complete integral if we can find the roots of* $B(x) = 0$.

In the middle of the nineteenth century two algorithms for computing the rational part of the primitive for $R(x)$ *without* factoring $B(x)$ were discovered. The first one was by C. Hermite [**166**] and was based on polynomial algebra and the second one was by M. W. Ostrogradsky [**240**] and was based on linear algebra. More recently, E. Horowitz [**176**] rediscovered the second method and discussed its complexity. The problem of computing the transcendental part of the primitive is usually credited to M. Rothstein [**260**] and B. M. Trager [**293**], with a technical refinement given by D. Lazard and R. Rioboo

[**197**]. This algorithm has been implemented in the current versions of the most widely used symbolic integrators. The Risch algorithm for integrating elementary functions (whenever possible) is based on generalizations of the Hermite reduction and the Rothstein-Trager algorithm. See the book by M. Bronstein [**80**] for details. The author wishes to thank M. Kauers for clarifying some of the historical aspects of these methods.

The integration of **rational functions** is the first challenging problem of elementary analysis. Given

$$R(x) := \frac{a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0}{b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0} \tag{8.7.1}$$

with a_i, $b_i \in \mathbb{R}$ and assuming conditions for the convergence of the integral, the problem is to obtain an analytic expression for

$$I_{n,m}(a,b;\mathbf{a},\mathbf{b}) := \int_a^b R(x)\,dx. \tag{8.7.2}$$

Here $\mathbf{a} := \{a_0,\, a_1, \ldots, a_n\}$ and $\mathbf{b} := \{b_0,\, b_1, \ldots, b_n\}$ are the coefficients of the integrand.

Normalization. In the case of a finite interval $[a,b]$, the integral in (8.7.2) may be normalized to the half-line $[0,\,\infty)$ by the transformation

$$x = \frac{bt+a}{1+t}, \tag{8.7.3}$$

which produces

$$\int_a^b R(x)\,dx = \int_0^\infty R_1(t)\,dt, \tag{8.7.4}$$

with a new rational integrand

$$R_1(t) = \frac{b-a}{(1+t)^2} R\left(\frac{bt+a}{1+t}\right). \tag{8.7.5}$$

If the original interval of integration is $(-\infty, a]$, the normalization is given by $t = a - x$. The change $t = x - b$ normalizes $[b, \infty)$. Finally, the identity

$$\int_{-\infty}^\infty R(x)\,dx = \int_0^\infty \left(R(x) + R(-x)\right)\,dx \tag{8.7.6}$$

normalizes the whole real line.

The normalization reduces the problem of integration of rational functions to that of

$$I_{n,m}(\mathbf{a},\mathbf{b}) = \int_0^\infty R(x)\,dx. \tag{8.7.7}$$

In the rest of the section it is assumed that the integral in (8.7.7) converges. This requires that $m-n \geq 2$ and that the polynomial

$$B(x) := b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0 \tag{8.7.8}$$

have no zeros on $[0,\infty)$.

8.7.1. The method of partial fractions. This section establishes a well-known elementary result.

Theorem 8.7.1. *Let $R(x) = A(x)/B(x)$ be a rational function. Assume that the roots of $B(x) = 0$ are known. Then the integral of R can be evaluated explicitly in terms of these roots.*

The discussion in the previous section shows that it suffices to consider the half-line $[0,\,\infty)$. The method of partial fractions converts the rational function $R(x) = A(x)/B(x)$ into a sum of the form

$$R(x) = \sum_{j=1}^{r} \frac{A_j}{(x-z_j)^{n_j}} + \sum_{j=1}^{s} \frac{B_j x + C_j}{(x^2+2u_jx+u_j^2+v_j^2)^{m_j}}. \tag{8.7.9}$$

The parameters z_j are the real roots of $B(x)=0$ and the n_j are the corresponding multiplicities. The complex roots appear as $u_j \pm iv_j$ and they have multiplicity m_j. In order to analyze the integral of R over $[0,\infty)$, the roots with multiplicity 1 are separated and R is written in the form given in Note 8.2.10.

Therefore the explicit integration of R over $[0,\infty)$ requires the analysis of six types of integrals, considered first over the finite interval $[0,N]$ to avoid a preliminary discussion of convergence.

Type 1.

$$I_1(N;w) := \int_0^N \frac{dx}{x-w}, \tag{8.7.10}$$

with $w<0$. This type corresponds to (negative) simple real roots of the denominator of the integrand. The value of I_1 can be computed in elementary terms and is given by

$$I_1(N;w) = \ln(N-w) - \ln(-w). \tag{8.7.11}$$

Observe that $I_1(N;w)$ diverges as $N \to \infty$.

Type 2.

$$I_2(N;w,m) := \int_0^N \frac{dx}{(x-w)^m}, \tag{8.7.12}$$

with $w<0$ and $m>1$. This type corresponds to (negative) real roots with multiplicity $m>1$. This can also be evaluated by elementary means to produce

$$I_2(N;w,m) = \frac{1}{1-m}\left(\frac{1}{(N-w)^{m-1}} - \frac{1}{(-w)^{m-1}}\right).$$

This integral converges to the finite value

$$I_{2,\infty}(w,m) = \lim_{N\to\infty} I_2(N;w,m) = \frac{1}{(m-1)(-w)^{m-1}}. \tag{8.7.13}$$

Type 3.

$$I_3(N;u,v) := \int_0^N \frac{(2x+2u)\,dx}{x^2+2ux+u^2+v^2}, \tag{8.7.14}$$

with u, $v \in \mathbb{R}$. This is also elementary and it is given by

$$I_3(N;u,v) = \ln\left(\frac{N^2+2uN}{u^2+v^2}+1\right). \tag{8.7.15}$$

Observe that $I_3(N;u,v)$ diverges as $N \to \infty$.

Type 4.

$$I_4(N;u,v,m) := \int_0^N \frac{(2x+2u)\,dx}{(x^2+2ux+u^2+v^2)^m}, \tag{8.7.16}$$

with u, $v \in \mathbb{R}$ and $m>1$. This integral has the value

$$I_4(N;u,v,m) = -\frac{1}{m-1}\left(\frac{1}{(N^2+2uN+u^2+v^2)^{m-1}} - \frac{1}{(u^2+v^2)^{m-1}}\right).$$

Therefore

$$I_{4,\infty}(u,v,m) = \lim_{N\to\infty} I_4(N;u,v,m) = \frac{1}{(m-1)(u^2+v^2)^{m-1}}.$$

Type 5.

$$I_5(N; u, v) := \int_0^N \frac{dx}{x^2 + 2ux + u^2 + v^2}, \tag{8.7.17}$$

with u, $v \in \mathbb{R}$ and $v > 0$. This integral is given by

$$I_5(N; u, v) = \frac{1}{v}\left(\tan^{-1}\left(\frac{N+u}{v}\right) - \tan^{-1}\left(\frac{u}{v}\right)\right). \tag{8.7.18}$$

As $N \to \infty$, this becomes

$$I_{5,\infty}(u, v) = \lim_{N\to\infty} I_5(N; u, v) = \frac{1}{v}\left(\frac{\pi}{2} - \tan^{-1}\left(\frac{u}{v}\right)\right).$$

Type 6.

$$I_6(N; u, v, m) := \int_0^N \frac{dx}{(x^2 + 2ux + u^2 + v^2)^m}, \tag{8.7.19}$$

with u, $v \in \mathbb{R}$ and $m > 1$. The evaluation of this integral as $N \to \infty$ is presented next. To simplify the notation, rewrite the integrand in (8.7.19).

Theorem 8.7.2. *Let $n \in \mathbb{N}$ and define $D = 4(ac - b^2)/ac$. Assume $a \neq 0$, $b \geq 0$, and $cD > 0$. Then*

$$\begin{aligned}\int_0^\infty & \frac{dx}{(ax^2 + 2bx + c)^{n+1}} \\ &= \frac{2\binom{2n}{n}}{a(cD)^{n+1}} \times \left\{\sqrt{acD}\cot^{-1}\left(\frac{2b}{\sqrt{acD}}\right) - b\sum_{j=1}^{n} \frac{D^j}{j\binom{2j}{j}}\right\}.\end{aligned}$$

Proof. Start with the case $n = 1$:

$$\int_0^\infty \frac{dx}{ax^2 + 2bx + c} = \frac{1}{\sqrt{ac - b^2}} \cot^{-1}\left(\frac{b}{\sqrt{ac - b^2}}\right). \tag{8.7.20}$$

This is evaluated by completing the square and a simple trigonometric substitution:

$$\begin{aligned}\int_0^\infty \frac{dx}{ax^2 + 2bx + c} &= \frac{1}{a}\int_{b/a}^\infty \frac{du}{u^2 - d/a^2} \\ &= \frac{1}{\sqrt{-D}}\int_{b/\sqrt{-D}}^\infty \frac{dv}{v^2 + 1}.\end{aligned}$$

Differentiating (8.7.20) with respect to c produces

$$\int_0^\infty \frac{dx}{(ax^2+2bx+c)^n} = \frac{(-1)^{n-1}}{(n-1)!}\frac{\partial^{n-1}}{\partial c^{n-1}}\left[\frac{\cot^{-1}(b/\sqrt{ac-b^2})}{\sqrt{ac-b^2}}\right].$$

Now let $h(a,b,c)$ be the integral in (8.7.20). Observe that

$$h(a^2, abc, b^2) = h(1,b,1)/ac. \tag{8.7.21}$$

In the formula stated in the theorem, change the parameters sequentially as $a \mapsto a^2$, $c \mapsto c^2$, $b \mapsto abc$. In the new format, both sides satisfy the differential-difference equation

$$-2nc(1-b^2)f_{n+1} = \frac{df_n}{dc} + \frac{b}{ac^{2n}}. \tag{8.7.22}$$

The result is obtained by reversing the transformations of parameters indicated above. □

Corollary 8.7.3. *Using the notation of Theorem* 8.7.2, *it follows that*

$$\sum_{j=1}^\infty \frac{D^j}{j\binom{2j}{j}} = \frac{\sqrt{acD}}{b}\cot^{-1}\left(\frac{2b}{\sqrt{acD}}\right). \tag{8.7.23}$$

Note 8.7.4. The case of $b=0$ corresponds to **Wallis' formula** discussed in Chapter 9.

Note 8.7.5. The exact value of $I_6(N;u,v,m)$ will not be required. Its limiting value as $N \to \infty$ is given in Theorem 8.7.2. It states that

$$I_{6,\infty}(u,v,m) := \lim_{N\to\infty} I_6(N;u,v,m) \tag{8.7.24}$$

is given by

$$\begin{aligned} I_{6,\infty}(u,v,m) &= \int_0^\infty \frac{dx}{(x^2+2ux+u^2+v^2)^m} \\ &= \frac{2\binom{2m-2}{m-1}}{(2v)^{2m}} \times \left\{ 2v\tan^{-1}\left(\frac{v}{u}\right) - u\sum_{k=1}^{m-1}\frac{(2v)^{2k}}{k\binom{2k}{k}(u^2+v^2)^k}\right\}. \end{aligned}$$

Example 8.7.6. The method described here is illustrated with the evaluation of the integral of the rational function

$$R(x) = \frac{(x-1)^2(x+3)^2(x^2+x+1)}{(x+2)^2(x^2+x+2)(x^2+4x+5)^2}. \tag{8.7.25}$$

The discussion starts with the decomposition of $R(x)$ in partial fractions in the form

$$\begin{aligned} R(x) &= \frac{27}{4}\frac{1}{(x+2)^2} + \frac{117}{16}\frac{1}{x+2} + \frac{1}{144}\frac{1-45x}{x^2+x+2} \\ & -\frac{2}{3}\frac{17x+53}{(x^2+4x+5)^2} - \frac{7}{9}\frac{9x+25}{x^2+4x+5}. \end{aligned}$$

This can be transformed into the format described in the previous analysis. The result is

$$\begin{aligned} R(x) &= \frac{27}{4}\frac{1}{(x+2)^2} + \frac{117}{16}\frac{1}{x+2} - \frac{5}{32}\frac{2x+1}{x^2+x+2} + \frac{47}{288}\frac{1}{x^2+x+2} \\ & -\frac{17}{3}\frac{2x+4}{(x^2+4x+5)^2} - \frac{38}{3}\frac{1}{(x^2+4x+5)^2} - \frac{7}{2}\frac{2x+4}{x^2+4x+5} \\ & -\frac{49}{9}\frac{1}{x^2+4x+5}. \end{aligned}$$

Now integrate each term over $(0, N)$ and let $N \to \infty$ in those pieces that have a finite limit. The eight parts follow.

Part 1.

$$\int_0^\infty \frac{dx}{(x+2)^2} = I_{2,\infty}(-2,2) = \frac{1}{2}.$$

Part 2.

$$\int_0^N \frac{dx}{x+2} = I_1(N,-2) = \ln(N+2) - \ln 2.$$

Part 3.

$$\int_0^N \frac{2x+1}{x^2+x+2}\,dx = I_3\left(N, \frac{1}{2}, \frac{\sqrt{7}}{2}\right) = \ln(N^2+N+2) - \ln 2.$$

Part 4.

$$\int_0^\infty \frac{dx}{x^2+x+2} = I_{5,\infty}\left(\frac{1}{2}, \frac{\sqrt{7}}{2}\right) = \frac{2}{\sqrt{7}}\left(\frac{\pi}{2} - \tan^{-1}(1/\sqrt{7})\right).$$

Part 5.

$$\int_0^\infty \frac{2x+4}{(x^2+4x+5)^2} = I_{4,\infty}(2,1;2) = \frac{1}{5}.$$

Part 6.

$$\int_0^\infty \frac{dx}{(x^2+4x+5)^2} = I_{6,\infty}(2,1;2) = -\frac{1}{5} + \frac{1}{2}\tan^{-1}\left(\frac{1}{2}\right).$$

Part 7.

$$\int_0^N \frac{2x+4}{x^2+4x+5}\,dx = I_3(N;2,1) = \ln(N^2+4N+5) - \ln 5.$$

Part 8.

$$\int_0^\infty \frac{dx}{x^2+4x+5} = I_{5,\infty}(2,1) = \frac{\pi}{2} - \tan^{-1}(2).$$

Combining these values gives

$$\begin{aligned}
&\int_0^\infty R(x)\,dx \\
&= \frac{191}{40} + \left(\frac{47}{288\sqrt{7}} - \frac{49}{18}\right)\pi - \frac{19}{3}\tan^{-1}\left(\frac{1}{2}\right) + \frac{49}{9}\tan^{-1} 2 \\
&- \frac{47}{144\sqrt{7}}\tan^{-1}\left(\frac{1}{\sqrt{7}}\right) - \frac{229}{32}\ln 2 + \frac{7}{2}\ln 5 \\
&+ \lim_{N\to\infty}\left[\frac{117}{16}\ln(N+2) - \frac{5}{32}\ln(N^2+N+2) - \frac{7}{2}\ln(N^2+4N+5)\right].
\end{aligned}$$

The reader can check that the limit vanishes and can use the relations

$$\tan^{-1} 2 + \tan^{-1}\frac{1}{2} = \frac{\pi}{2} \quad \text{and} \quad \tan^{-1}\sqrt{7} + \tan^{-1}\frac{1}{\sqrt{7}} = \frac{\pi}{2}$$

to write the final result as

$$\begin{aligned}
&\int_0^\infty R(x)\,dx = \\
&\quad \frac{191}{40} - \frac{106}{9}\tan^{-1}\left(\frac{1}{2}\right) + \frac{47}{144\sqrt{7}}\tan^{-1}\sqrt{7} - \frac{229}{32}\ln 2 + \frac{7}{2}\ln 5.
\end{aligned}$$

Conclusion. We have an explicit method to evaluate the integral of a rational function $R(x) = A(x)/B(x)$ *provided* the factorization of B is given. The convergence of the integral shows that the divergent parts, coming from integrals of type 1 and type 3, must be grouped together to produce the final result.

8.8. Symbolic integration. The methods of Hermite and Rothstein-Trager

This section considers algorithms for the evaluation of the integral of a rational function $R(x) = A(x)/B(x)$ developed by Hermite. Details and extensions may be found in M. Bronstein's book [**80**] and in S. Boettner's thesis [**57**].

It will be assumed that the condition deg $A <$ deg B is satisfied. This can be achieved by dividing A by B. The method is based on the **square-free factorization** of the denominator $B(x)$. The description of the method begins with some preliminaries on polynomials. The coefficients are taken from a field $\mathbb{K}$ such as $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$. These fields are examples of **fields of characteristic zero**. All discussions of unique factorization presented below need to assume the proviso *except for constant factors.*

Note 8.8.1. Given two polynomials A, B, the largest common divisor will be denoted by $\gcd(A, B)$. This is defined uniquely up to a scalar multiple. Therefore, the statement $\gcd(A, B) = 1$ is to be interpreted to mean that the largest common divisor is a polynomial of degree 0.

Definition 8.8.2. A complex polynomial $p \in \mathbb{K}(x)$ is called **irreducible** if every factorization $p = p_1 \cdot p_2$ implies p_1 or p_2 is constant. Otherwise, the polynomial is called **reducible**.

Example 8.8.3. The fundamental theorem of algebra implies that every irreducible polynomial over $\mathbb{C}$ is linear.

Theorem 8.8.4. *Let $p \in \mathbb{K}[x]$ be a polynomial. Then p may be written as a product of irreducible factors. This decomposition is unique aside from the order of the factors.*

Proof. Proceed by induction on the degree of p. If p is irreducible, the statement is valid. Otherwise, there are polynomials p_1, p_2 such that $p = p_1p_2$, with deg p_1 and deg p_2 less than deg p. This proves the existence of the decomposition. The uniqueness is left to the reader to verify. □

The theorem shows that every polynomial p can be expressed in the form

$$p = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}, \tag{8.8.1}$$

with p_i irreducible, $p_i \neq p_j$ for $i \neq j$, and $a_i \in \mathbb{N}$.

Exercise 8.8.5. Let p_1, p_2 be distinct irreducible polynomials. Prove that $\gcd(p_1, p_2) = 1$.

Definition 8.8.6. A polynomial p is called **square-free** if there is no polynomial g, with $\deg g > 0$, such that $p = g^2 h$.

Exercise 8.8.7. Check that an irreducible polynomial is square-free but that the converse is not true. Prove also that a finite product of distinct irreducible polynomials is square-free.

Exercise 8.8.8. Let $p \in \mathbb{K}[x]$. Prove that f is square-free if and only if $\gcd(p, p') = 1$.

In the decomposition (8.8.1) let

$$q_i = \prod_{1 \leq j \leq r} \{p_j \, : \, a_j = i\}.$$

Then the q_i are square-free polynomials that are relatively prime.

Definition 8.8.9. Let $p \in \mathbb{K}[x]$. The **square-free decomposition** of p is the representation of the form

$$p = q_1 \cdot q_2^2 \cdot q_3^3 \cdots q_m^m, \tag{8.8.2}$$

where the polynomials q_i are pairwise relatively prime square-free. This decomposition is unique.

Algorithm for the computation of the square-free decomposition of a polynomial. The next algorithm provides a method to compute the polynomials q_i in (8.8.2) using only gcd operations. Assume that p has the representation (8.8.2). Then compute

$$E_1 := \gcd(p, p') \tag{8.8.3}$$

to obtain $E_1 = q_2 \cdot q_3^2 \cdots q_m^{m-1}$. Now divide p by E_1 to obtain

$$E_2 = \frac{p}{E_1} = q_1 \cdot q_2 \cdots q_m. \tag{8.8.4}$$

In the next step, compute

$$E_3 := \gcd(E_1, E_1') \tag{8.8.5}$$

to obtain $E_3 = q_3 \cdot q_4^2 \cdots q_m^{m-2}$. Now compute

$$E_4 = \frac{E_1}{E_3} = q_2 \cdot q_3 \cdots q_m. \tag{8.8.6}$$

Then q_1 is obtained as E_2 divided by E_4. The algorithm is now restarted with the polynomial E_1.

Hermite reduction. This method reduces the integral of a rational function to one with a square-free denominator.

Start with a square-free factorization of the denominator $B(x)$ in the form

$$B = \prod_{i=1}^{m} q_i^i. \tag{8.8.7}$$

Let $w = q_1 \cdot q_2^2 \cdots q_{m-1}^{m-1}$. Then $\gcd(q_m' w, q_m) = 1$. The Euclidean algorithm gives polynomials a, b such that

$$(1-m)aq_m' w + bq_m = A. \tag{8.8.8}$$

Now since

$$\begin{aligned} \left(\frac{a}{q_m^{m-1}}\right)' &= \frac{a' q_m^{m-1} - (m-1)aq_m^{m-2}q_m'}{q_m^{2m-2}} \\ &= \frac{a'}{q_m^{m-1}} + \frac{(1-m)aq_m'}{q_m^m}, \end{aligned}$$

it follows that

$$\begin{aligned} \frac{A}{B} &= \frac{(1-m)aq_m' w + bq_m}{q_m^m\, w} \\ &= \frac{(1-m)aq_m'}{q_m^m} + \frac{b}{q_m^{m-1} w} + \frac{a'}{q_m^{m-1}} - \frac{a'}{q_m^{m-1}} \\ &= \left(\frac{a}{q_m^{m-1}}\right)' + \frac{b + a'w}{q_m^{m-1} w} \end{aligned}$$

and this gives

$$\int \frac{A}{B}\, dx = \frac{a}{q_m^{m-1}} + \int \frac{b + a'w}{q_m^{m-1} w}\, dx. \tag{8.8.9}$$

Thus the integral of A/B has been expressed as a rational function plus the integral of a new rational function where no factor of the denominator appears with a power greater than $m-1$. Iterating this procedure gives the next theorem. This is the **Hermite reduction theorem**.

Theorem 8.8.10. *Let R be a rational function. Then there are rational functions R_1, R_2 with the denominator of R_2 square-free such that*

$$\int R(x)\,dx = R_1(x) + \int R_2(x)\,dx.$$

Example 8.8.11. Consider the integral

$$\int \frac{dx}{(x^2+1)(x+1)^2}.$$

The square-free decomposition of the denominator consists of $q_1 = x^2+1$ and $q_2 = x+1$. The Euclidean algorithm gives

$$1 = \frac{1}{2}(x^2+1) + \frac{1-x}{2}(x+1),$$

so that $a = -\frac{1}{2}$ and $b = \frac{1}{2}(1-x)$. Therefore

$$\int \frac{dx}{(x+1)^2(x^2+1)} = -\frac{\frac{1}{2}}{x+1} + \int \frac{\frac{1}{2}(1-x)}{(x^2+1)(x+1)}\,dx.$$

The method of Rothstein and Trager. This method evaluates the integral of a reduced rational function with square-free denominator. The method was developed by M. Rothstein [**259, 260, 261**] and B. M. Trager [**293, 294**].

The procedure begins with the partial fraction decomposition

$$R(x) = \frac{A(x)}{B(x)} = \sum_{i=1}^{n} \frac{\lambda_i}{x-x_i}$$

where $\{x_1, x_2, \ldots, x_n\}$ are the roots of B and

$$\lambda_i = \lim_{x\to x_i} (x-x_i)R(x)$$

is called the **residue** of R at x_i.

Exercise 8.8.12. Check that $\lambda_i = A(x_i)/B'(x_i)$. Recall that $B'(x_i)$ $\neq 0$ since B is square-free.

The previous exercise shows that knowledge of the roots of B determines the residues. The real question is how to proceed without knowing the roots. One of the key tools is the **resultant** of two polynomials. This is discussed in the next note.

Note 8.8.13. Given two polynomials $A(x) = a_n x^n + \cdots + a_0$ and $B(x) = b_m x^m + \cdots + b_0$ with roots α_i and β_j, respectively ($1 \leq i \leq n$, $1 \leq j \leq m$), the **resultant** is defined by

$$\operatorname{Res}(A, B) = a_n^m b_m^n \prod_{i=1}^{n} \prod_{j=1}^{m} (\alpha_i - \beta_j)\,.$$

Therefore A and B have a common root if and only if $\operatorname{Res}(A, B) = 0$.

The resultant can be computed as the determinant of the **Sylvester matrix**. This is shown in the case of $n = 4$ and $m = 3$ for simplicity:

$$\operatorname{Sylv}(A, B) = \begin{pmatrix} a_4 & a_3 & a_2 & a_1 & a_0 & 0 & 0 \\ 0 & a_4 & a_3 & a_2 & a_1 & a_0 & 0 \\ 0 & 0 & a_4 & a_3 & a_2 & a_1 & a_0 \\ b_3 & b_2 & b_1 & b_0 & 0 & 0 & 0 \\ 0 & b_3 & b_2 & b_1 & b_0 & 0 & 0 \\ 0 & 0 & b_3 & b_2 & b_1 & b_0 & 0 \\ 0 & 0 & 0 & b_3 & b_2 & b_1 & b_0 \end{pmatrix}.$$

Exercise 8.8.14. Check that up to a scalar, the resolvent of A and A' is the discriminant of A introduced in Chapter 4.

The next result rephrases the condition for a rational function to have a pole with a prescribed residue.

Proposition 8.8.15. *Let $R = A/B$ be a rational function with square-free denominator. Then R has a pole at x_i with residue λ_i if and only if*

$$B(x_i) = 0 \quad \textit{and} \quad A(x_i) - \lambda_i B'(x_i) = 0.$$

Therefore the residues λ_i are those values λ such that $B(x)$ and $A(x) - \lambda B'(x)$ have a common root at x_i. Note 8.8.13 states that these roots can be computed in terms of the resultant

$$r(\lambda) = \operatorname{resultant}_x(B, A - \lambda B'). \tag{8.8.10}$$

This is a polynomial in λ and its roots give the values of the residues for R.

Let $\lambda_1, \ldots, \lambda_n$ be the distinct roots of $r(\lambda) = 0$. For each λ_i, the expression $\gcd(B, A - \lambda_i B')$ is a polynomial whose roots are exactly the places where A/B has residue λ_i. The final expression for the integral is

$$\int \frac{A(x)}{B(x)}\,dx = \sum_{r(\lambda)=0} \lambda \ln \gcd(B, A - \lambda B'). \tag{8.8.11}$$

Exercise 8.8.16. Check that these polynomials do not need to be factored any further since the factors would belong to logarithms with a common coefficient.

Example 8.8.17. Example 8.8.11 is now completed using the method of Rothstein and Trager. The missing integral is

$$\frac{1}{2}\int \frac{1-x}{x^3+x^2+x+1}\,dx.$$

The first step is to evaluate the resultant

$$r(\lambda) = \text{resultant}_x(x^3+x^2+x+1, 1-x-\lambda(3x^2+2x+1))$$

as the determinant of the Sylvester matrix

$$\begin{aligned} r(\lambda) &= \det \begin{bmatrix} 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 \\ -3\lambda & -2\lambda-1 & -\lambda+1 & 0 & 0 \\ 0 & -3\lambda & -2\lambda-1 & -\lambda+1 & 0 \\ 0 & 0 & -3\lambda & -2\lambda-1 & -\lambda+1 \end{bmatrix} \\ &= -16(\lambda-1)(\lambda+\tfrac{1}{2})^2. \end{aligned}$$

Therefore only the residues $\lambda_1 = 1$ and $\lambda_2 = -\frac{1}{2}$ occur. The corresponding polynomials are computed by $\gcd(B, A - \lambda B')$. This gives

$$\gcd(x^3+x^2+x+1, 1-x-(3x^2+2x+1)) = x+1$$

and

$$\gcd(x^3+x^2+x+1, 1-x+\tfrac{1}{2}(3x^2+2x+1)) = x^2+1.$$

It follows that

$$\int \frac{1-x}{x^3+x^2+x+1}\,dx = \ln(x+1) - \frac{1}{2}\ln(x^2+1).$$

The original integral is evaluated as

$$\int \frac{dx}{(x+1)^2(x^2+1)} = -\frac{\frac{1}{2}}{x+1} + \frac{1}{2}\ln(x+1) - \frac{1}{4}\ln(x^2+1).$$

Exercise 8.8.18. Use the methods described here to confirm the evaluation

$$\int \frac{dx}{(x^2-2)(x+3)^2} = -\frac{1}{7(x+3)} + \frac{6}{49}\ln(x+3) \\ + \frac{1}{98}\left(\frac{11}{\sqrt{2}} - 6\right)\ln(\sqrt{2}-x) - \frac{1}{98}\left(\frac{11}{\sqrt{2}} + 6\right)\ln(\sqrt{2}+x).$$

Is it possible to express the answer without the number $\sqrt{2}$?

Exercise 8.8.19. Check that the integral

$$I_n = \int \frac{dx}{(x^2-2)(x+3)^2(x+1)^n}$$

is of the form

$$R_n(x) + A_n\ln(\sqrt{2}-x) + B_n\ln(\sqrt{2}+x) + C_n\ln(1+x) + D_n\ln(x+3)$$

where R_n is a rational function and A_n, B_n, C_n, D_n are numbers of the form $x+\sqrt{2}y$ with $x,\ y \in \mathbb{Q}$. Experiment and predict arithmetic properties of these coefficients. For example, the length of the period of the continued fractions of these numbers seems to have interesting behavior.

Chapter 9

Wallis' Formula

9.1. An experimental approach

The integral considered here is

$$W_m = \int_0^\infty \frac{dx}{(x^2+1)^{m+1}}, \quad m \in \mathbb{N}_0. \tag{9.1.1}$$

This is one of the simplest examples for which one can produce a closed-form evaluation. It is also an example that permits us to illustrate a variety of techniques developed in the evaluation of more difficult integrals. An equivalent formulation of this integral in terms of an infinite product is one of the first analytic expressions for π; see Section 12.6. The exponent is chosen as $m+1$ and not m to produce a cleaner form of the final answer.

In order to predict a closed-form formula for W_m, a list of values is produced using `Mathematica`. The values of W_m for $1 \leq m \leq 10$ are

$$\left\{ \frac{\pi}{4}, \frac{3\pi}{16}, \frac{5\pi}{32}, \frac{35\pi}{256}, \frac{63\pi}{512}, \frac{231\pi}{2048}, \frac{429\pi}{4096}, \frac{6435\pi}{65536} \frac{12155\pi}{131072}, \frac{46189\pi}{524288} \right\}.$$

It is clear from this data that W_m is a rational multiple of π. Further examination of the data shows that the denominator is always a power of 2. The list of the corresponding exponents, that is,

$$a_m = -\nu_2\left(\frac{W_m}{\pi}\right) \tag{9.1.2}$$

(where $\nu_2(x)$ is the 2-adic valuation of x) is given by

$$\{2,\ 4,\ 5,\ 8,\ 9,\ 11,\ 12,\ 16,\ 17,\ 19\}\,. \tag{9.1.3}$$

It looks like the exponent a_m is bounded by $2m$. This leads to the definition

$$b_m = 2^{2m}W_m/\pi. \tag{9.1.4}$$

The values of b_m for $1 \leq m \leq 10$ are given by

$$\{1,\ 3,\ 10,\ 35,\ 126,\ 462,\ 1716,\ 6435,\ 24310,\ 92378\}\,. \tag{9.1.5}$$

At this point an option to produce a guess for the coefficients b_m is to consult the database produced by Neil Sloane in

`http://oeis.org/`

that contains an incredible amount of useful information. Inserting the first four values of the previous list, Sloane's database returns

$$b_m = \binom{2m-1}{m-1} = \frac{1}{2}\binom{2m}{m}. \tag{9.1.6}$$

This yields the guess

$$W_m = \frac{\pi}{2^{2m+1}}\binom{2m}{m}. \tag{9.1.7}$$

It is now desirable to prove this statement.

A second approach to guessing the form of b_m is to compute symbolically several values of the sequence b_m and to consider their prime factorization. For instance, the factorization of

$$b_{100} = 45274257328051640582702088538742081937252294837706668420660$$

contains a number of consecutive primes in decreasing order starting at 200; the factorization looks like

$$b_{100} = 199 \times 197 \times 193 \times 191 \times \cdots \times 5 \times 3 \times 2^2. \tag{9.1.8}$$

The presence of the consecutive primes suggests dividing b_{100} by 200!. It turns out that $200!/b_{100}$ is an integer with prime factorization of the form

$$\frac{200!}{b_{100}} = 97^2 \times 89^2 \times 83^2 \times 79^2 \times \cdots \times 5^{48} \times 3^{96} \times 2^{195}. \tag{9.1.9}$$

This form now suggests considering

$$\frac{200!}{b_{100} \cdot 100!^2}. \tag{9.1.10}$$

`Mathematica` shows that this number is 2. Naturally this could be a coincidence. Repeating the procedure shows that

$$\frac{(2m)!}{b_m \cdot m!^2} = 2 \tag{9.1.11}$$

for every tested value of m. This is consistent with (9.1.6).

9.2. A proof based on recurrences

The goal of this section is to provide a proof of the formula predicted in the previous section.

Theorem 9.2.1 (Wallis' formula). *Let $m \in \mathbb{N}_0$. Then*

$$W_m = \int_0^\infty \frac{dx}{(x^2+1)^{m+1}} = \frac{\pi}{2^{2m+1}} \binom{2m}{m}. \tag{9.2.1}$$

Proof. The first step is to produce a recurrence for W_m. This comes from the identity

$$\begin{aligned} \frac{1}{(x^2+1)^{m+1}} &= \frac{x^2+1}{(x^2+1)^{m+2}} \\ &= \frac{2x}{(x^2+1)^{m+2}} \cdot \frac{x}{2} + \frac{1}{(x^2+1)^{m+2}} \\ &= \frac{x}{2} \cdot \frac{d}{dx} \left(-\frac{1}{m+1} \frac{1}{(x^2+1)^{m+1}} \right) + \frac{1}{(x^2+1)^{m+2}}. \end{aligned}$$

Integrate to produce

$$W_m = -\frac{1}{m+1} \int_0^\infty \frac{x}{2} \cdot \frac{d}{dx} \frac{1}{(x^2+1)^{m+1}} \, dx + W_{m+1}. \tag{9.2.2}$$

Integrate by parts to obtain

$$W_{m+1} = \frac{2m+1}{2(m+1)} W_m. \tag{9.2.3}$$

This is the desired recurrence. To prove the theorem, it suffices to check that the right-hand side of (9.2.1) satisfies the same recurrence. In order to achieve this, define

$$Y_m = \frac{2^{2m+1}}{\pi \binom{2m}{m}} W_m \tag{9.2.4}$$

and substituting in (9.2.3) yields

$$Y_{m+1} = Y_m. \tag{9.2.5}$$

The value $Y_0 = 1$ shows that $Y_m = 1$ as claimed. □

9.3. A proof based on generating functions

The generating function of the central binomial coefficients is given in Theorem 2.7.3 as

$$\sum_{k=0}^{\infty} \binom{2k}{k} u^k = \frac{1}{\sqrt{1-4u}}. \tag{9.3.1}$$

Wallis' formula is now multiplied by t^m and summed from $m = 0$ to infinity. This yields

$$\sum_{m=0}^{\infty} \int_0^{\infty} \frac{t^m \, dx}{(x^2+1)^{m+1}} = \frac{\pi}{2} \sum_{m=0}^{\infty} \left(\frac{t}{4} \right)^m \binom{2m}{m}. \tag{9.3.2}$$

The integrand on the left-hand side can be summed as a geometric progression to produce the elementary integral

$$\int_0^{\infty} \frac{dx}{x^2+1-t} = \frac{\pi}{2} \frac{1}{\sqrt{1-t}}. \tag{9.3.3}$$

Equation (9.3.3) is used as a starting point to produce a proof of Wallis' formula.

Lemma 9.3.1. *Let $m \in \mathbb{N}$ and let*

$$(a)_m = a(a+1)(a+2)\cdots(a+m-1)$$

be the Pochhammer symbol. Then

$$\left(\frac{d}{dt} \right)^m (x-t)^{-a} = (a)_m (x-t)^{-a-m}.$$

Proof. The induction step is

$$\begin{aligned}\frac{d}{dt}\left[\left(\frac{d}{dt}\right)^m (x-t)^{-a}\right] &= \frac{d}{dt}\left[(a)_m\,(x-t)^{-a-m}\right]\\ &= (a)_m(-1)(x-t)^{-a-m-1}(-a-m)\\ &= (a)_m(a+m)(x-t)^{-a-m-1}.\end{aligned}$$

The result follows from $(a)_m(a+m) = (a)_{m+1}$. □

To establish Wallis' formula, start with (9.3.3) in the form

$$\int_0^\infty (x^2+1-t)^{-1}\,dx = \frac{\pi}{2}(1-t)^{-1/2} \tag{9.3.4}$$

and differentiate m times with respect to t. The statement in the lemma gives

$$\int_0^\infty (1)_m(x^2+1-t)^{-1-m}\,dx = \frac{\pi}{2}(1/2)_m(1-t)^{-1/2-m}.$$

Now put $t=0$ to obtain

$$\int_0^\infty \frac{dx}{(x^2+1)^{m+1}} = \frac{\pi}{2}\frac{(1/2)_m}{(1)_m}.$$

The result now follows from $(1)_m = m!$ and

$$\left(\frac{1}{2}\right)_m = \frac{(2m)!}{m!\,2^{2m}}. \tag{9.3.5}$$

Exercise 9.3.2. Check the details.

9.4. A trigonometric version

Wallis' formula is expressed in trigonometric form by the change of variables $x = \tan\theta$ in (9.1.1). This produces

$$W_m = \int_0^{\pi/2} \cos^{2m}\theta\,d\theta. \tag{9.4.1}$$

To obtain a recurrence for W_m, write

$$\cos^{2m}\theta = (\cos\theta)^{2m-2}\,(1-\sin^2\theta) \tag{9.4.2}$$

and integrate to obtain

$$W_m = W_{m-1} + \frac{1}{2m-1}\int_0^{\pi/2} \sin\theta\,\frac{d}{d\theta}\cos^{2m-1}\theta\,d\theta. \tag{9.4.3}$$

Integrate by parts to produce

$$W_m = W_{m-1} - \frac{1}{2m-1} W_m. \tag{9.4.4}$$

This is equivalent to (9.2.3).

A second recurrence based on a trigonometric form. The trigonometric form

$$W_m = \int_0^{\pi/2} \cos^{2m} \theta \, d\theta \tag{9.4.5}$$

is now employed to produce a new recurrence for W_m.

The double angle formula $\cos^2 \theta = \frac{1}{2}(1 + \cos 2\theta)$ produces

$$\begin{aligned} W_m &= \frac{1}{2^m} \int_0^{\pi/2} (1 + \cos 2\theta)^m \, d\theta \\ &= \frac{1}{2^{m+1}} \int_0^{\pi} (1 + \cos x)^m \, dx \\ &= \frac{1}{2^{m+1}} \sum_{j=0}^{m} \binom{m}{j} \int_0^{\pi} \cos^j x \, dx \end{aligned}$$

where the change of variables $x = 2\theta$ was employed to produce the second line.

Observe that by symmetry

$$\int_0^{\pi} \cos^j x \, dx = 0 \quad \text{for } j \text{ odd} \tag{9.4.6}$$

and

$$\int_0^{\pi} \cos^j x \, dx = 2 \int_0^{\pi/2} \cos^j x \, dx \quad \text{for } j \text{ even.} \tag{9.4.7}$$

Therefore, with $j = 2k$,

$$W_m = \frac{1}{2^m} \sum_{k=0}^{\lfloor \frac{m}{2} \rfloor} \binom{m}{2k} \int_0^{\pi/2} \cos^{2k} x \, dx, \tag{9.4.8}$$

which produces the desired recurrence:

Theorem 9.4.1. *The integral W_m satisfies the recurrence*

$$W_m = \frac{1}{2^m} \sum_{k=0}^{\lfloor \frac{m}{2} \rfloor} \binom{m}{2k} W_k \tag{9.4.9}$$

for $m \geq 1$. This is supplemented by the initial condition $W_0 = \frac{\pi}{2}$.

To prove Wallis' formula, employ the **intelligent guess** given in (9.2.1). Inserting the formula for W_m in (9.2.1) into (9.4.9) shows the equivalence stated in the next proposition.

Proposition 9.4.2. *The recurrence* (9.4.9) *follows from the binomial sum identity*

$$\sum_{k=0}^{\lfloor \frac{m}{2} \rfloor} 2^{-2k} \binom{m}{2k} \binom{2k}{k} = 2^{-m} \binom{2m}{m}. \tag{9.4.10}$$

Observe that in the sum in (9.4.10) the index k can be extended for all $k \geq 0$ since those $k \geq \lfloor \frac{m}{2} \rfloor$ give a zero contribution.

Proposition 9.4.3. *The binomial sum identity*

$$\sum_{k=0}^{\infty} 2^{-2k} \binom{m}{2k} \binom{2k}{k} = 2^{-m} \binom{2m}{m} \tag{9.4.11}$$

holds. This implies the recurrence for the integral W_m.

Proof. The proof of (9.4.11) is based on generating functions. It is now shown that

$$\sum_{m=0}^{\infty} \left(\sum_{k=0}^{\infty} 2^{-2k} \binom{m}{2k} \binom{2k}{k} \right) t^m = \sum_{m=0}^{\infty} 2^{-m} \binom{2m}{m} t^m.$$

The right-hand side is simply

$$\sum_{m=0}^{\infty} \binom{2m}{m} \left(\frac{t}{2} \right)^m = \frac{1}{\sqrt{1-2t}}$$

according to Theorem 2.7.3. The left-hand side is now written as

$$\sum_{m=0}^{\infty} \left(\sum_{k=0}^{\infty} 2^{-2k} \binom{m}{2k} \binom{2k}{k} \right) t^m = \sum_{k=0}^{\infty} 2^{-2k} \binom{2k}{k} \left(\sum_{m=0}^{\infty} \binom{m}{2k} t^m \right).$$

Now employ the result of Exercise 2.11.11

$$\sum_{m=0}^{\infty} \binom{m}{j} t^m = \frac{t^j}{(1-t)^{j+1}}$$

to simplify the left-hand side to

$$\begin{aligned}\sum_{k=0}^{\infty} 2^{-2k} \binom{2k}{k} \frac{t^{2k}}{(1-t)^{2k+1}} &= \frac{1}{1-t} \sum_{k=0}^{\infty} \binom{2k}{k} \left(\frac{t^2}{4(1-t)^2} \right)^k \\ &= \frac{1}{1-t} \frac{1}{\sqrt{1 - t^2/(1-t)^2}}.\end{aligned}$$

This reduces to $1/\sqrt{1-2t}$ and the identity has been established. □

9.5. An automatic proof

The identity (9.4.11) can be established automatically by the methods developed by H. Wilf and D. Zeilberger. The command

$$ct(binomial(m, 2i) binomial(2i, i) 2^{-2i}, 1, i, m, N),$$

entered in the WZ-package produces the recurrence

$$f(m+1) = \frac{2m+1}{m+1} f(m)$$

for the left-hand side of (9.4.11). The proof is finished by checking that $2^{-m}\binom{2m}{m}$ satisfies the same recurrence and that the initial data agree.

Note 9.5.1. Let

$$c(m) := \frac{2^{4m+1}}{2m+1} \binom{2m}{m}^{-2}.$$

Then Wallis' inequality is the statement

$$\frac{2m}{2m+1} \leq \frac{c(m)}{\pi} \leq 1, \quad m \geq 0. \tag{9.5.1}$$

Wallis' infinite product is an immediate consequence of this inequality.

In the paper by P. Paule and V. Pillwein [**243**] the reader will find an automatic proof of (9.5.1) and of the improved versions

$$\frac{4m+1}{4m+2} \le \frac{c(m)}{\pi} \le \frac{4m+2}{4m+3}, \quad m \ge 0,$$

obtained originally by J. Gurland [**155**] and also of

$$\frac{32m^2+32m+7}{4(2m+1)(4m+3)} \le \frac{c(m)}{\pi} \le \frac{16(m+1)(2m+1)}{32m^2+56m+25}, \quad m \ge 0.$$

Chapter 10

Farey Fractions

10.1. Introduction

The previous chapters have described trees that illustrate arithmetical properties of sequences. In this chapter the set of rational numbers is given a similar discrete representation. The reader will find additional material related to the topic of this chapter in the preliminary version of the book by A. Hatcher [**161**].

10.2. Farey fractions and the Stern-Brocot tree

The starting point is to associate to $\mathbb{Q} \cap [0, 1]$ a collection of sequences determined by the denominators. The assumption is that every rational number $x \in [0, 1]$ is written in reduced form; that is, numerator and denominator are relatively prime. This determines the denominator of x uniquely.

Definition 10.2.1. The **Farey sequence** $\mathfrak{F}_n$ **of order** n is the ascending sequence of all rational numbers in $[0, 1]$ whose denominator is at most n. The elements of $\mathfrak{F}_n$ are called **Farey fractions**.

Example 10.2.2. The Farey sequence of order 4 is

$$\mathfrak{F}_4 = \left\{ \frac{0}{1}, \frac{1}{4}, \frac{1}{3}, \frac{1}{2}, \frac{2}{3}, \frac{3}{4}, \frac{1}{1} \right\}.$$

Naturally $\mathfrak{F}_n \subset \mathfrak{F}_{n+1}$ and

$$\mathbb{Q} \cap [0,1] = \bigcup_{n=1}^{\infty} \mathfrak{F}_n. \tag{10.2.1}$$

Proposition 10.2.3. *Let $n \in \mathbb{N}$ and let*

$$\varphi(n) = |\{j \in \mathbb{N} : 1 \leq j \leq n \textit{ and } \gcd(j,n) = 1\}|$$

be the ***Euler totient function****. Then*

$$|\mathfrak{F}_n| = 1 + \varphi(1) + \varphi(2) + \cdots + \varphi(n).$$

Proof. Let $j \in \mathbb{N}$ and let $1 \leq j \leq n$. If $\gcd(j,n) \neq 1$, then the fraction j/n reduces to one with smaller denominator. Therefore j/n is already part of some $\mathfrak{F}_i$ with $i < n$. The fractions $j/n \in \mathfrak{F}_n$ appearing for the first time at this level are precisely those with $\gcd(j,n) = 1$. The extra 1 in the formula accounts for $x = 0$. □

Exercise 10.2.4. Prove that for $n > 1$, the cardinality of $\mathfrak{F}_n$ is an odd number with $1/2$ appearing as the middle term of $\mathfrak{F}_n$.

The properties of fractions adjacent in the Farey sequence are discussed next.

Definition 10.2.5. Two fractions a/b and c/d in a Farey sequence are said to be **adjacent Farey fractions** if they occur in consecutive order in some Farey sequence.

Exercise 10.2.6. Check that $7/10$ and $5/7$ are adjacent Farey fractions.

Lemma 10.2.7. *No two adjacent Farey fractions can have the same denominator.*

Proof. The pair $(x-1)/n$ and x/n cannot be adjacent since

$$\frac{x-1}{n} < \frac{x-1}{n-1} < \frac{x}{n}.$$

□

Definition 10.2.8. Let a/b, c/d be fractions in reduced terms. Their **mediant** is defined by

$$\frac{a}{b} \oplus \frac{c}{d} = \frac{a+c}{b+d}. \tag{10.2.2}$$

Note 10.2.9. The mediant is recognized as the manner in which scores are tabulated in games: two versions of the same game are played and a player scores a points from a possible total of b on the first game c out of d in the next try. The record for both tries is $a+c$ out of $b+d$ chances.

It is clear that the mediant is a rational number strictly between a/b and c/d. Some elementary properties of Farey fractions are described next.

Lemma 10.2.10. *If $ad - bc = 1$ and $c/d < a/b$, then $\frac{a}{b} \oplus \frac{c}{d}$ is the unique fraction with smallest possible denominator in the interval $(c/d,\, a/b)$.*

Proof. Suppose that $c/d < u/v < a/b$ and $u/v \leq (a+c)\,/\,(b+d)$. Then $(a+c)\,/\,(b+d) - c/d \geq u/v - c/d$, and it follows that $v \geq (b+d)\,(ud - cv) \geq b+d$. Similarly, if $(a+c)\,/\,(b+d) \leq u/v$, from $a/b - (a+b)\,/\,(c+d) \geq a/b - u/v$ it follows that $v \geq (b+d)\,(av - bu) \geq b+d$. The uniqueness follows from Lemma 10.2.7. □

Lemma 10.2.11. *Two reduced fractions a/b, c/d are adjacent Farey fractions if and only if $|ad - bc| = 1$.*

Proof. If $|ad - bc| = 1$, Lemma 10.2.10 shows that no fraction between a/b and c/d has denominator smaller than $b + d > \max(b, d)$, and so $a/b, c/d$ are adjacent Farey fractions of order $\max(b, d)$.

To prove the converse, proceed by induction and assume that for any adjacent Farey fractions $a/b, c/d$ of order $n-1$, the identity $|ad - bc| = 1$ holds. Any Farey fraction in $\mathfrak{F}_n$ that is not already in $\mathfrak{F}_{n-1}$ must have n as denominator. Denote it by x/n. Find two adjacent Farey fractions $c/d < a/b$ of order $n-1$ such that $c/d < x/n < a/b$. Lemma 10.2.7 implies that $c/d, x/n$ and $x/n, a/b$ are adjacent Farey fractions of order n. Lemma 10.2.10 implies that $x = a + c$, $n = b + d$, and so $xd - cn = (a+c)\,d - c\,(b+d) = ad - bc = 1$, and $an - bx = a\,(b+d) - b\,(a+c) = ad - bc = 1$. □

Exercise 10.2.12. Explore properties of the differences between two consecutive Farey fractions. The picture in Figure 10.2.1 gives these values for $\mathfrak{F}_{100}$. The first and last points are not shown in the graph; they are much larger than the rest.

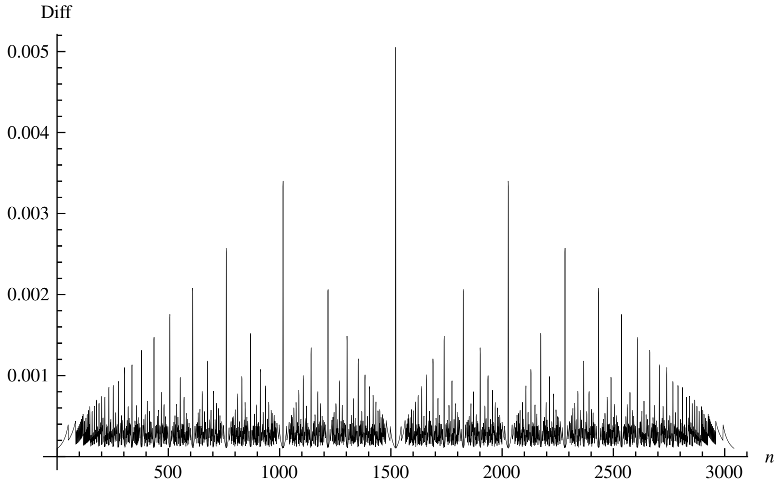


Figure 10.2.1. Difference among consecutive Farey fractions.

Finding approximations. An interesting application of Farey sequences is to find the rational number that approximates a given irrational number to within a given tolerance and that has the smallest possible denominator. That is, given an irrational number α and a tolerance $\epsilon > 0$, it is desired to obtain a fraction p/q such that $|\alpha - p/q| < \epsilon$ and $q > 0$ is as small as possible.

For example, consider the problem of finding p/q such that $|\pi - p/q| < 0.001$. For this example, observe that in the Farey sequence $\mathfrak{F}_{57}$ the numbers $\frac{179}{57} - 3$ and $\frac{22}{7} - 3$ are consecutive, that $\frac{179}{57} < \pi < \frac{22}{7}$, and that $\pi - \frac{179}{57} \sim 0.0012$ and $\frac{22}{7} - \pi \sim 0.0013$. Therefore no fraction with denominator less than or equal to 57 is close enough, and the desired fraction will appear in a later Farey sequence and it will be in the interval $\left(\frac{179}{57}, \frac{22}{7}\right)$. The next fraction to appear in this interval is the mediant $\frac{179+22}{57+7} = \frac{201}{64}$, and this in fact has $\pi - \frac{201}{64} \sim 0.00097$, so this is the desired fraction.

Mathematica has a function Rationalize that claims to perform this operation, but it seems inconsistent. For instance, in the example discussed here it correctly states

$$\texttt{Rationalize}[\mathrm{Pi}, 0.001] = \frac{201}{64},$$

but it gives

$$\texttt{Rationalize}[\mathrm{Pi}, 0.1] = \frac{22}{7},$$

when in fact $\frac{16}{5}$ is within the tolerance and has a smaller denominator.

Construction of the Stern-Brocot tree. The next step is to provide a representation of $\mathbb{Q} \cap [0,1]$ in terms of a binary tree. The process starts with the inductive definition of an increasing sequence of finite subsets of $\mathbb{Q} \cap [0,\, 1]$.

This sequence starts with

$$\mathcal{A}_{-1} = \{0/1, 1/1\} = \{0,1\}\,. \tag{10.2.3}$$

Observe that the elements of $\mathcal{A}_{-1}$ are adjacent (they form the complete set $\mathfrak{F}_1$).

Once $\mathcal{A}_n$ has been defined, $\mathcal{A}_{n+1}$ is obtained by adding to $\mathcal{A}_n$ all the mediants of consecutive fractions in $\mathcal{A}_n$. For example

$$\mathcal{A}_0 = \{0/1, (0+1)\,/\,(1+1)\,, 1/1\} = \{0, 1/2, 1\}\,. \tag{10.2.4}$$

Exercise 10.2.13. Prove that $|\mathcal{A}_n| = 2^{n+1}+1$ for $n \geq -1$.

Exercise 10.2.14. Prove that each pair of consecutive fractions in $\mathcal{A}_n$ is a pair of adjacent Farey fractions of order at most F_{n+3}. Here F_n is the nth Fibonacci number. Prove also that $\mathcal{A}_n$ contains a fraction with denominator F_{n+3}.

The set $\mathbb{Q} \cap [0,\, 1]$ is now partitioned using the sets $\mathcal{A}_n$. Define $\mathcal{B}_{-1} = \mathcal{A}_{-1} = \{0,1\}$ and for $n \geq 0$ let $\mathcal{B}_n = \mathcal{A}_n \backslash \mathcal{A}_{n-1}$. The sets $\mathcal{B}_n$ are clearly disjoint and $|\mathcal{B}_n| = 2^n$ for $n \geq 0$.

The elements in $\mathcal{B}_n$ are interpreted as the children of the elements of $\mathcal{A}_{n-1}$. Two parents a/b and c/d have the mediant $(a+c)/(b+d)$ as their child. At time $n=-1$ there are two parents $\{0/1, 1/1\}$ with a single child $\{1/2\}$ at time $n=0$. The two children at time $n=1$ are $\{1/3, 2/3\}$ coming from a parent at generation $n=-1$ and a parent at generation $n = 0$. At time $n = 2$ there are four children $\{1/4, 2/5, 3/5, 3/4\}$.

The successive generations $\mathcal{B}_n$ are depicted by a binary tree by drawing an edge from a fraction u/v in $\mathcal{B}_{n-1}$ to a fraction x/y in $\mathcal{B}_n$ precisely when x/y is a child of u/v.

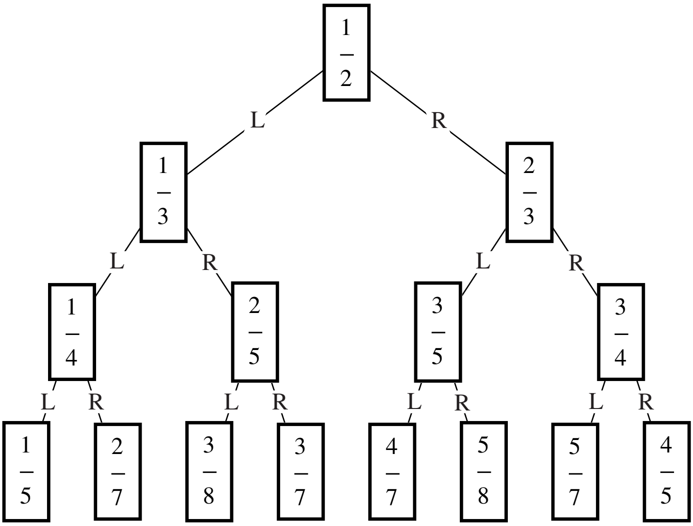


Figure 10.2.2. The Stern-Brocot tree.

The edge from x/y to u/v is labeled L if $x/y < u/v$, and R if $x/y > u/v$.

Exercise 10.2.15. Verify that

$$\mathcal{B}(4)=\left\{\frac{1}{6}, \frac{2}{9}, \frac{3}{11}, \frac{3}{10}, \frac{4}{11}, \frac{5}{13}, \frac{5}{12}, \frac{4}{9}, \frac{5}{9}, \frac{7}{12}, \frac{8}{13}, \frac{7}{11}, \frac{7}{10}, \frac{8}{11}, \frac{7}{9}, \frac{5}{6}\right\}.$$

Compute the descendents of 4/7 in $\mathcal{B}(4)$.

Lemma 10.2.16. *There is a bijective correspondence between the fractions in $\mathcal{B}_n$ and the finite words of length n over the symbols L, R (the notation is meant to represent left or right turns), with the empty word e representing the root of the tree $\{1/2\}$. By convention the infinite words L^∞ and R^∞ represent 0 and 1, respectively.*

Note 10.2.17. The notation $Q(w)$ is employed for the rational number corresponding to the finite word w. For example, $Q(e) = 1/2$ and $Q(RLR) = 5/8$.

Definition 10.2.18. If p is a fraction in $\mathcal{B}_n$, denote by p^-, p^+ the left and right parents of p, respectively, so that $p = p^- \oplus p^+$ and $p^- < p < p^+$. For example, if $p = 5/14$, then $p^- = 1/3$ and $p^+ = 4/11$. The notation is extended to finite words, so that w^- is the word that satisfies $Q(w^-) = p^-$ and $Q(w^+) = p^+$.

Exercise 10.2.19. Check the following properties:

(1) The word w^- is obtained from w by deleting all terminal L's (if any) and then deleting one R. Similarly, w^+ is obtained from w by deleting all terminal R's (if any), then deleting one L.

(2) If $p \in \mathcal{B}_n$, precisely one of p^-, p^+ is in $\mathcal{B}_{n-1}$.

(3) Each pair $(p^-, p), (p^-, p^+), (p, p^+)$ is a pair of adjacent Farey fractions.

(4) Any two fractions $a/b, c/d$ in $[0,1]$ with $|ad - bc| = 1$ occur as a pair of adjacent Farey fractions in some $\mathcal{A}_n$.

It has been established that Q provides a bijective correspondence between the rational numbers in $(0,1)$ and the finite words over the symbols L and R. The next exercise describes the connection between a word w and the continued fraction expansion of $Q(w)$.

Exercise 10.2.20. Given a finite word w, define a finite sequence of positive integers $(a_1, a_2, \ldots, a_k)$ as follows. Prepend an extra L at the beginning of w, and then append to w an extra copy of its last letter. Let the terms of the sequence $(a_1, a_2, \ldots, a_k)$ count the number of consecutive blocks of L's or R's in the modified word. For example, the word $LRLL$ is modified to $LLRLLL$, and it gives the sequence $(0, 2, 1, 3)$, and the word $RRLRRR$ gives the sequence $(0, 1, 2, 1, 4)$. Prove that $(0, a_1, a_2, \ldots, a_k)$ is the continued fraction expansion of $Q(w)$. **Note:** The convention employed here is that the continued fraction of a number in $[0,1]$ starts with 0.

10.3. The distribution of denominators

The goal of this section is to describe properties of the denominators of the rational number $Q(w)$ in terms of those of the word w. The results presented here appeared in the paper by D. Baney, S. Beslin, and V. De Angelis [**39**].

Proposition 10.3.1. *The numbers $Q(wR^n)$ increase to $Q(w^+)$ and the numbers $Q(wL^n)$ decrease to $Q(w^-)$.*

Proof. Let $N(w)$ denote the denominator of $Q(w)$ and let $|w|$ be the length of w. Observe that $N(w) \geq |w| + 2$ and $N(wR) = N(w) + N(w^+)$. Now, the numbers $Q(w)$ and $Q(w^+)$ are adjacent Farey fractions; therefore

$$Q(w^+) - Q(w) = \frac{1}{N(w)N(w^+)}.$$

It follows that

$$Q(w^+) - Q(wR^n) = \frac{1}{N(w^+)(N(w) + nN(w^+))}$$

for all n. The result now follows from the inequalities

$$Q(w^-) < Q(wL) < Q(w) < Q(wR) < Q(w^+).$$

□

Exercise 10.3.2. Prove that for any word u of length m, the inequalities

$$Q\left(wLu\right) < Q\left(wLR^m\right) < Q\left(\left(wL\right)^+\right) = Q\left(w\right)$$

hold. Interpret these inequalities in terms of the effect of making a left turn in a walk on the Stern-Brocot tree. **Hint:** Compare the values of $Q(LRLR)$ and $Q(LRLRLw)$ for an arbitrary word.

The next step is to consider infinite words over $\{L, R\}$. The following notation is employed: if $w = x_1x_2\cdots$ is such a word, let $w_n = x_1x_2\cdots x_n$ be the finite word consisting of the initial block of length n of w.

Exercise 10.3.3. Let w be an arbitrary word over $\{L, R\}$. Prove that $Q(w_n)$ is a Cauchy sequence in $[0, 1]$.

Exercise 10.3.4. Prove that every irrational number in $[0,1]$ has a unique representation as an infinite word over $\{L,R\}$ and that every rational number has two such representations.

Algorithm for smallest denominator. The Stern-Brocot tree is now used to describe an algorithm to find the rational number of the smallest possible denominator $N(\alpha,\ \beta)$ between two given numbers $\alpha,\ \beta \in [0,1]$. First represent both α and β as infinite paths on the Stern-Brocot tree. If there is more than one choice (that is, if at least one of $\alpha,\ \beta$ is rational), choose a pair of representations that have the longest possible initial overlap. Then $N(\alpha,\beta)$ is the last common ancestor on the paths. This algorithm is illustrated with an example. Let $\alpha = 3/8$, $\beta = 5/13$. Then α corresponds to $LRLRL^\infty$ and $LRLLR^\infty$, and β corresponds to $LRLRRL^\infty$ and $LRLRLR^\infty$. The maximum overlap occurs for the pairs $LRLRL^\infty$, $LRLRLR^\infty$, with initial overlap $LRLRL$. Therefore

$$N(3/8,5/13) = Q(LRLRL) = 8/21.$$

This procedure is essentially equivalent to the algorithm of Section II of the paper by S. J. Beslin, D. J. Baney, and V. De Angelis [**51**].

Note 10.3.5. The same algorithm can be explained from the point of view of continued fractions. Let $[a_1, a_2, \ldots]$ and $[b_1, b_2, \ldots]$ be the expansions for α and β. If an expansion is finite, attach ∞ at the end. For instance, the expansions for $7/19$ are $[0,2,1,2,2,\infty]$ and $[0,2,1,2,1,1,\infty]$. Define

$$d = d(\alpha,\beta) = \min\{k : a_k \neq b_k\}, \quad m = m(\alpha,\beta) = \min\{a_d, b_d\},$$

and $M(\alpha,\beta) = m + \sum_{i=1}^{d-1} a_i$, so that $M(\alpha,\beta) - 1$ is the length of the overlap of the corresponding paths on the Stern-Brocot tree. Choose a pair of expansions that maximizes $M(\alpha,\beta)$. Then $N(\alpha,\beta)$ is given by the continued fraction $[a_1, a_2, \ldots, a_{d-1}, m+1]$. This procedure is essentially equivalent to the algorithm of Section III of [**51**].

As example, $3/8$ has expansions $[0,2,1,1,1,\infty]$ and $[0,2,1,2,\infty]$, and $5/13$ has expansions $[0,2,1,1,2,\infty]$ and $[0,2,1,1,1,1,\infty]$. The maximum value for M is 6 and occurs for the pairs $[0,2,1,1,1,\infty]$ and

$[0,2,1,1,1,1,\infty]$. Then, as before, $N(3/8,5/13) = [0,2,1,1,1,2] = 8/21$.

Exercise 10.3.6. Prove that the above algorithm works.

Let $\mathbb{T} := \{(\alpha, \beta) : 0 < \alpha \leq 1; 0 \leq \beta < \alpha\}$ be the lower part of the unit square. Assume that the pair (α, β) is chosen randomly inside $\mathbb{T}$. Given $n \in \mathbb{N}$, what is the probability that the denominator of $N(\alpha, \beta)$ is n?

Exercise 10.3.7. Let $n \geq 2$ and $0 < k < n$ with $\gcd(n,k) = 1$. Prove that there are unique integers a, b such that $a < n$, $0 \leq b < k$, and $ak - bn = 1$.

Let w be a finite word over $\{L, R\}$. Define the rectangle

$$\mathcal{R}(w) = (Q(w), Q(w^+)] \times [Q(w^-), Q(w)) \subset \mathbb{T}.$$

Lemma 10.3.8. *If $w \neq u$, then $\mathcal{R}(w) \cap \mathcal{R}(u) = \emptyset$.*

Proof. For any word w, Proposition 10.3.1 gives

$$Q(w^-) = \lim_{n\to\infty} Q(wL^n) = Q(wL^\infty)$$

and

$$Q(wL^\infty) < Q(wL) < Q(w) < Q(wR) < Q(wR^\infty) = \lim_{n\to\infty} Q(wR^n).$$

The last step is provided by

$$\lim_{n\to\infty} Q(wR^n) = Q(w^+).$$

Assume without loss of generality that $Q(w) < Q(u)$. Suppose first that w is not a subword of u and u is not a subword of w. Then there are (possibly empty) words v, s, t such that $w = vLs$, $u = vRt$, and it follows that

$$Q(w^+) = Q(vLsR^\infty) \leq Q(vLR^\infty) = Q(v) < Q(u),$$

so that $(Q(w), Q(w^+)] \cap (Q(u), Q(u^+)] = \emptyset$.

Suppose now that u is a subword of w. Then $w = uLv$ for some word v, and

$$Q(w^+) = Q(uLvR^\infty) \leq Q(uLR^\infty) = Q(u),$$

and this gives $(Q(w), Q(w^+)] \cap (Q(u), Q(u^+)] = \emptyset$, as before. The case where w is a subword of u is similar. □

Lemma 10.3.9. *Let α, $\beta \in \mathbb{R}$, with $0 < \alpha \le 1$, $0 \le \beta < \alpha$. Then there is a finite word w such that $(\alpha, \beta) \in \mathcal{R}(w)$, and $Q(w)$ is the fraction with the lowest possible denominator between α and β.*

Proof. Let u, v be words such that $Q(u) = \alpha$, $Q(v) = \beta$. If u is not a subword of v and v is not a subword of u, let w be the first common ancestor of u and v. Then $u = wRs$, $v = wLt$ for some words s, t that do not end in L^∞ or R^∞. This shows that $Q(w^-) < Q(w) < Q(w)$, $Q(w) < Q(u) < Q(w^+)$ and it follows that $(\alpha, \beta) = (Q(u), Q(v)) \in \mathcal{R}(w)$. On the other hand, if v is a subword of u, then v agrees with u on at most a finite number of symbols. Choose an infinite word v' such that $Q(v') = Q(v)$ and the words v', u have maximum possible overlap w. Since $Q(u) > Q(v)$, it must be that $u = wRt$ and $v = wLs$ for some words t and s. Then $Q(w) < Q(wRt) \le Q(wR^\infty) = Q(w^+)$, and $Q(w^-) = Q(wL^\infty) \le Q(wLs) < Q(w)$, i.e., $(\alpha, \beta) = (Q(u), Q(v)) \in \mathcal{R}(w)$. The case that u is a subword of v is similar, and the last assertion follows from the algorithm described above. □

Lemmas 10.3.8 and 10.3.9 show that $\{\mathcal{R}(w) : w \in B_n, n \ge 0\}$ is a partition of the triangle $\{(\alpha, \beta) : 0 < \alpha \le 1, 0 \le \beta < \alpha\}$, as shown in Figure 10.3.1. The rectangles in the partition have been labeled with the corresponding smallest denominator.

Lemma 10.3.10. *There is a bijection θ between the set*

$$\{(n, k) : n \ge 2, \quad 0 < k < n, \quad \gcd(n, k) = 1\} \tag{10.3.1}$$

and the set of finite words over $\{L, R\}$, given by $\theta(n, k) = w$, where $Q(w) = a/n$, $Q(w^-) = b/k$, and a, b are such that $ak - bn = 1$, $0 < a < n$, $0 \le b < k < n$.

Proof. This comes directly from the proof of Lemma 10.3.7. □

Proposition 10.3.11. *Let $n \ge 2$, $0 < k < n$ with $\gcd(n, k) = 1$ be given, let $w = \theta(n, k)$, and let a, b be such that $ak - bn = 1$, as in Lemma* 10.3.7. *Then for any α, β with $0 < \alpha \le 1$, $0 \le \beta < \alpha$, the*

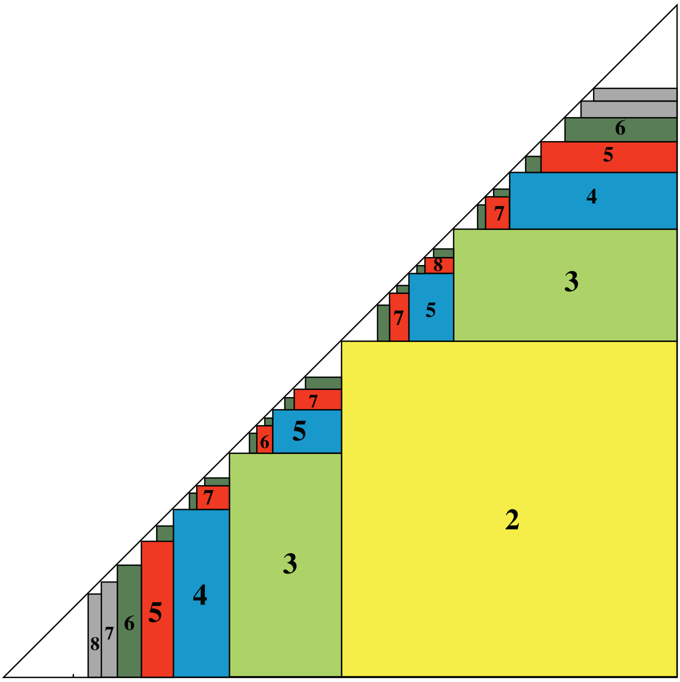


Figure 10.3.1. The rectangles

fraction with smallest possible denominator between α *and* β *is* a/n *if and only if* $(\alpha, \beta) \in \mathcal{R}(w)$.

Proof. Suppose that the fraction with the lowest denominator between α and β is a/n. If $(b-a)/(n-k) < \alpha$, then it would follows that $\beta < a/n < (b-a)/(n-k) < \alpha$, a contradiction. Therefore, it must be that $a/n = Q(w) < \alpha \leq (b-a)/(n-k) = Q(w^+)$, and in a similar fashion $Q(w^-) \leq \beta < Q(w)$, i.e., $(\alpha, \beta) \in \mathcal{R}(w)$. The converse is Lemma 10.3.9. □

Theorem 10.3.12. *Choose the point* (α, β) *randomly from the triangle* $\mathbb{T} = \{(\alpha, \beta) : 0 < \alpha \leq 1, 0 \leq \beta < \alpha\}$, *with uniform distribution. Then the probability that the smallest possible denominator of any* *fraction between α and β is n is given by*

$$\frac{4}{n^3}\sum_{\substack{k<n;\\ \gcd(k,n)=1}}\frac{1}{k}.$$

Proof. The area of $\mathbb{T}$ is $1/2$. Proposition 10.3.11 shows that the probability in question is

$$2\sum \text{area of } \mathcal{R}(w) = 2\sum(Q(w^+)-Q(w))(Q(w)-Q(w^-)),$$

where the sum is over all words w such that $Q(w)=a/n$ for some a relatively prime to n. Using the bijective correspondence described after Lemma 10.3.9, it follows that $Q(w^-)=b/k$, where $0\le b<k<n$, $ak-bn=1$, and then by definition $Q(w^+)=(a-b)/(n-k)$. Then

$$\begin{aligned}\frac{1}{2}\sum \text{ area of } \mathcal{R}(w) &= \sum_{\substack{k<n;\\ \gcd(k,n)=1}}\left(\frac{a-b}{n-k}-\frac{a}{n}\right)\left(\frac{a}{n}-\frac{b}{k}\right)\\ &= \sum_{\substack{k<n;\\ \gcd(k,n)=1}}\frac{1}{n(n-k)}\frac{1}{nk}\\ &= \frac{1}{n^3}\sum_{\substack{k<n;\\ \gcd(k,n)=1}}\left(\frac{1}{k}+\frac{1}{n-k}\right)\\ &= \frac{2}{n^3}\sum_{\substack{k<n;\\ \gcd(k,n)=1}}\frac{1}{k}.\end{aligned}$$

This establishes the result. □

The sum over all the probabilities computed above gives the next identity.

Corollary 10.3.13.

$$\sum_{n=2}^{\infty}\frac{4}{n^3}\sum_{\substack{k<n;\\ \gcd(k,n)=1}}\frac{1}{k}=1.$$

The next exercise was shown to the author by S. Northshield.

Exercise 10.3.14. Use the formulas

$$\sum_{n=1}^{\infty} \sum_{\substack{k<n;\\ \gcd(k,n)=1}} \frac{1}{n^m k} = \frac{1}{\zeta(m+1)} \sum_{n=1}^{\infty} \sum_{k=1}^{n} \frac{1}{n^m k},$$

$$\sum_{n=1}^{\infty} \sum_{k=1}^{n} \frac{1}{n^2 k} = 2\zeta(3) \quad \text{and} \quad \sum_{n=1}^{\infty} \sum_{k=1}^{n} \frac{1}{n^3 k} = \frac{5}{4}\zeta(4)$$

to obtain a new derivation of Corollary 10.3.13. Then show that the expected value of $N(\alpha, \beta)$ is 4. Here ζ is the Riemann zeta function described in Chapter 16.

Chapter 11

The Exponential Function

11.1. Introduction

This chapter considers the first transcendental function encountered in analysis. This is the **exponential function** e^x and is also considered part of the family of **elementary functions**. The definition is given in terms of **power series** and a short review of these is given first. In the previous chapters the concept of **generating function** has been employed. This is simply a formal mechanism to describe the operation on sequences. In this chapter the question of actual convergence of the series is discussed. A large part of the chapter is dedicated to the number e: one of the basic constants of mathematics. It even has its own book by E. Maor [**210**].

11.1.1. Functions defined by power series. The concept of power series is introduced first.

Definition 11.1.1. Let $\mathbb{N}_0 := \mathbb{N} \cup \{0\}$ and let $\{a_n : n \in \mathbb{N}_0\}$ be a sequence of real numbers. For $x \in \mathbb{R}$ define the polynomial

$$f_n(x) := \sum_{j=0}^{n} a_j x^j. \tag{11.1.1}$$

For each $x \in \mathbb{R}$ fixed, $\{f_n(x) : n \in \mathbb{N}_0\}$ is a sequence of real numbers. Let $X \subset \mathbb{R}$ be the set of $x \in \mathbb{R}$ for which this sequence converges. The set X depends on the sequence $\{a_n\}$. For $x \in X$, define the function

$$f(x) = \lim_{n\to\infty} f_n(x). \tag{11.1.2}$$

The function f is called **the power series associated to the sequence** $\{a_n\}$. The polynomials $f_n(x)$ are called the **partial sums** of f.

Example 11.1.2. Exercise 1.5.17 states the formula for a geometric progression

$$1 + x + x^2 + \cdots + x^n = \frac{1 - x^{n+1}}{1 - x} \tag{11.1.3}$$

for $x \neq 1$. The closed-form expression for the partial sum shows that these sums converge precisely when $|x| < 1$. This defines the function

$$f(x) \equiv \sum_{j=0}^{\infty} x^j = \frac{1}{1-x}, \quad \text{for}|x| < 1. \tag{11.1.4}$$

Exercise 11.1.3. Prove that the sequence $\{x^n : n \in \mathbb{N}_0\}$ has a limit precisely when $-1 < x \leq 1$. The case of $x \neq 1$ follows from **Bernoulli's inequality**

$$(1+t)^n \geq 1 + nt \tag{11.1.5}$$

valid for $n \in \mathbb{N}_0$ and $t \in \mathbb{R}$ with $t \geq -1$.

The next theorem summarizes properties of functions defined by power series.

Theorem 11.1.4. *The power series*

$$f(x) = \sum_{j=0}^{\infty} a_j x^j \tag{11.1.6}$$

satisfies the following:

(1) *The set of points $X \subset \mathbb{R}$ where the series* (11.1.6) *converges contains an interval of the form $(-R, R)$. The maximum number R is called the* ***radius of convergence*** *of f. The extreme cases of $R = 0$ and $R = \infty$ are included. The full set of convergence X is the interval*

$(-R, R)$ together with some $(= 0,\ 1,\ 2)$ *of the endpoints $x = -R$ and $x = R$.*

(2) *The radius of convergence R can be obtained from the coefficients $\{a_j\}$ by*

$$R = \lim_{j\to\infty} \frac{|a_j|}{|a_{j+1}|} \tag{11.1.7}$$

or by

$$R = \lim_{j\to\infty} |a_j|^{-1/j}, \tag{11.1.8}$$

provided the limits exist.

(3) *For $x \in (-R, R)$ the function f is differentiable. Moreover its derivative is obtained by differentiating* (11.1.6) *term by term to produce*

$$f'(x) = \sum_{j=1}^{\infty} j a_j x^{j-1}. \tag{11.1.9}$$

The radius of convergence of the new series (11.1.9) *is also R.*

Exercise 11.1.5. Prove that the radius of convergence of the series for $(1-x)^{-a}$ given in Theorem 2.4.2 is 1.

The main function of this chapter is defined next.

Definition 11.1.6. The **exponential function** is defined by the power series

$$\exp(x) = \sum_{j=0}^{\infty} \frac{x^j}{j!}. \tag{11.1.10}$$

Exercise 11.1.7. Check that the radius of convergence is $R = \infty$. Therefore $\exp(x)$ is defined for all $x \in \mathbb{R}$.

Note 11.1.8. The elementary properties of this function will be described in this chapter. In particular, the famous number e is introduced as the limit of a sequence. It is then established that

$$\exp(x) = e^x. \tag{11.1.11}$$

The number e is one of the most important constants of analysis. The historical aspects of this number can be found in [**210**].

11.2. Elementary properties of the exponential function

This section provides a discussion of the exponential function. The properties are derived directly from the definition (11.1.10).

11.2.1. The addition theorem. The behavior of the exponential function under addition is established first.

Theorem 11.2.1. *The exponential function satisfies the* ***addition formula***

$$\exp(x+y) = \exp(x)\cdot\exp(y), \tag{11.2.1}$$

for all x, $y \in \mathbb{R}$.

Proof. Multiply the series defining $\exp(x)$ and $\exp(y)$ to produce

$$\sum_{j=0}^{\infty} \frac{x^j}{j!} \times \sum_{k=0}^{\infty} \frac{y^k}{k!} = \sum_{j,\,k=0}^{\infty} \frac{x^j y^k}{j!\,k!}.$$

The double sum is changed from indices j, k to j, n where n is the sum $n = j+k$. Then n runs over $\mathbb{N}_0$ and j satisfies $0 \leq j \leq n$. Therefore

$$\begin{aligned} \exp(x)\cdot\exp(y) &= \sum_{n=0}^{\infty}\sum_{j=0}^{n} \frac{x^j y^{n-j}}{j!\,(n-j)!} \\ &= \sum_{n=0}^{\infty} \frac{(x+y)^n}{n!}, \end{aligned}$$

by the binomial theorem. The last series is $\exp(x+y)$. □

Corollary 11.2.2. *For each $x \in \mathbb{R}$*

$$exp(x)\cdot exp(-x) = 1. \tag{11.2.2}$$

In particular $exp(x) \neq 0$.

11.2.2. The differential equation. Most readers' first encounter with the exponential function is due to the fact that its derivative is the same as the function. This property is employed next to establish additional properties.

Theorem 11.2.3. *The exponential function $f(x) = \exp(x)$ is the unique solution to the (differential) equation*

$$\begin{aligned} f'(x) &= f(x), \\ f(0) &= 1. \end{aligned} \tag{11.2.3}$$

Proof. The derivative of (11.1.10) is given by

$$f'(x) = \sum_{j=1}^{\infty} j \frac{x^{j-1}}{j!} = \sum_{j=1}^{\infty} \frac{x^{j-1}}{(j-1)!} = \sum_{j=0}^{\infty} \frac{x^j}{j!} = f(x).$$

The value $f(0) = 1$ is clear. This shows that $f(x) = \exp(x)$ satisfies the differential equation (11.2.3). To establish uniqueness, let $h(x)$ be another solution of (11.2.3). Define $h_1(x) = h(x)\exp(-x)$. Then

$$h_1'(x) = h'(x)\exp(-x) - h(x)\exp(-x) = 0. \tag{11.2.4}$$

This shows that $h_1(x)$ is constant. Evaluating at $x = 0$ gives the result. □

Exercise 11.2.4. Give a proof of the addition theorem using the differential equation. **Hint:** Define $h_1(x) = \exp(x+y)/\exp(y)$.

11.2.3. The exponential function is not rational.

The differential equation satisfied by the exponential function provides an elementary proof of the next result.

Theorem 11.2.5. *The exponential is not a rational function.*

Proof. Assume the existence of polynomials A and B, of degrees a and b, respectively, such that $e^x = A(x)/B(x)$. Theorem 11.2.3 yields

$$A'(x)B(x) - A(x)B'(x) = A(x)B(x).$$

This gives a contradiction since the left-hand side is a polynomial of degree at most $a+b-1$ and the right-hand side has degree $a+b$. □

Corollary 11.2.6. *There is no collection of numbers $a_0, a_1, \ldots, a_N$ of fixed length $N+1$ such that*

$$\frac{a_0}{n!} + \frac{a_1}{(n-1)!} + \cdots + \frac{a_N}{(n-N)!} = 0,$$

for all $n \in \mathbb{N}$.

Proof. The existence of such a set would imply a recurrence with constant coefficients for the sequence $\{1/n!\}$. Theorem 8.3.1 then implies that e^x is a rational function. This contradicts Theorem 11.2.5. □

11.3. The constant e

This section considers one of the basic constants of mathematics. Its role is only paralleled by π, described in Chapter 12. The definition employs the fact that an increasing sequence, bounded from above, has a limit in $\mathbb{R}$.

Definition 11.3.1. The number e is defined by the limit

$$e := \lim_{n\to\infty} (1 + 1/n)^n. \tag{11.3.1}$$

The proof of the existence of the limit above is based upon the two sequences

$$a_n = (1 + 1/n)^n \quad \text{and} \quad b_n = (1 + 1/n)^{n+1}. \tag{11.3.2}$$

The discussion employs Bernoulli's inequality stated in Exercise 11.1.3.

Now

$$\frac{a_n}{b_{n-1}} = \left(\frac{n^2-1}{n^2} \right)^n = \left(1 - \frac{1}{n^2} \right)^n > 1 - \frac{1}{n}$$

shows that $\{a_n\}$ is increasing. Indeed, $a_n > b_{n-1} \times \frac{n-1}{n} = a_{n-1}$. Similarly $\{b_n\}$ is decreasing, as shown by

$$\frac{b_{n-1}}{a_n} = \left(\frac{n^2}{n^2-1} \right)^n = \left(1 + \frac{1}{n^2-1} \right)^n > \left(1 + \frac{1}{n^2} \right)^n > 1 + \frac{1}{n}.$$

This produces $b_{n-1} > a_n \left(1 + \frac{1}{n}\right) = b_n$, as promised. It follows that $2 = a_1 < a_n < b_n < b_1 = 4$. The identity $b_n = a_n\left(1 + 1/n\right)$ shows that

$$\lim_{n\to\infty} a_n = \lim_{n\to\infty} b_n.$$

Note 11.3.2. The proof shows that $2 < e < 4$. Moreover, for each fixed $n \in \mathbb{N}$, the bounds

$$\left(1 + \frac{1}{n} \right)^n < e < \left(1 + \frac{1}{n} \right)^{n+1} \tag{11.3.3}$$

are valid. For example, $n=2$ gives $\frac{9}{4}<e<\frac{27}{8}$. These bounds will be improved in Exercise 11.3.4.

Exercise 11.3.3. Check that $n=5$ yields

$$\frac{7776}{3125}<e<\frac{46656}{15625} \tag{11.3.4}$$

and that this guarantees $2<e<3$.

Exercise 11.3.4. Read the paper by Y. Bicheng and L. Debnath [**54**] that establishes the inequality

$$\frac{1}{2(n+1)}<1-\frac{1}{e}\left(1+\frac{1}{n}\right)^n<\frac{3}{6n+5}, \tag{11.3.5}$$

for $n \geq 1$. In particular,

$$\lim_{n\to\infty} n\left(1-\frac{1}{e}\left(1+\frac{1}{n}\right)^n\right)=\frac{1}{2}. \tag{11.3.6}$$

Note 11.3.5. J. Sandor has established in [**265, 266**] the bounds

$$\left(1+\frac{1}{n}\right)^{n+a}<e<\left(1+\frac{1}{n}\right)^{n+b}.$$

The values $a=1/\ln 2-1$ and $b=1/2$ are the optimal choice of parameters.

11.4. The series representation of e

The constant e has been introduced by the limit

$$e=\lim_{n\to\infty}\left(1+\frac{1}{n}\right)^n. \tag{11.4.1}$$

In this section an alternative representation for e is established. The notation

$$e_n=\sum_{k=0}^{n}\frac{1}{k!} \tag{11.4.2}$$

is employed.

Theorem 11.4.1. *The number e is given by*

$$e=\sum_{k=0}^{\infty}\frac{1}{k!}. \tag{11.4.3}$$

In terms of the exponential function $\exp(x)$ *this states that* $e = \exp(1)$*. For* $n \in \mathbb{N}$*, the estimates*

$$0 < e - e_n < \frac{1}{n\,n!} \tag{11.4.4}$$

hold.

Proof. To check the identity between e and the series observe that

$$\begin{aligned} a_n &:= \left(1 + \frac{1}{n}\right)^n \\ &= 1 + \sum_{k=1}^{n} \frac{n(n-1)\cdots(n-k+1)}{k!\,n^k} \\ &= 1 + \sum_{k=1}^{n} \frac{1}{k!}\left(1 - \frac{1}{n}\right)\left(1 - \frac{2}{n}\right)\cdots\left(1 - \frac{k-1}{n}\right) \\ &\leq 1 + \sum_{k=1}^{n} \frac{1}{k!} = e_n \leq s. \end{aligned}$$

Therefore $e \leq s$. The opposite inequality is left as an exercise.

To prove (11.4.4), let s be the series in (11.4.3). Then $e_n \leq s = \lim_{n\to\infty} e_n$. Moreover

$$\begin{aligned} s - e_n = \sum_{k=n+1}^{\infty} \frac{1}{k!} &= \frac{1}{n!}\left(\frac{1}{n+1} + \frac{1}{(n+1)(n+2)} + \cdots\right) \\ &< \frac{1}{n!}\left(\frac{1}{n+1} + \frac{1}{(n+1)^2} + \cdots\right) \\ &= \frac{1}{n\,n!}, \end{aligned}$$

and (11.4.4) follows from here.

Exercise 11.4.2. Check the opposite inequality.

□

At this point there are two functions under consideration. The first one is the exponential function $\exp(x)$ defined by the power series in (11.1.10). The second one is the function e^x, whose value simply corresponds to exponentiation as described in Subsection 1.9.3. The next theorem states that these two functions are one and the same.

Theorem 11.4.3. *Let $x \in \mathbb{R}$. Then* $\exp(x) = e^x$.

A possible proof of this theorem is based on checking the identity for $x \in \mathbb{Q}$ and then extending it by continuity. The exercises give more details.

Exercise 11.4.4. Prove Theorem 11.4.3 by showing by induction that $\exp(n) = e^n$ for $n \in \mathbb{N}$. Extend it to $n \in \mathbb{Z}$ in a natural manner using the addition theorem. The extension to $\mathbb{Q}$ employs the identity

$$(\exp(m/n))^n = \exp(m). \tag{11.4.5}$$

Finally extend it to $x \in \mathbb{R}$ by approximating x by rational numbers.

Exercise 11.4.5. Introduce the polynomials

$$E_n(x) := \left(1 + \frac{x}{n}\right)^n \tag{11.4.6}$$

and check the relation

$$E_n'(x) = \frac{n}{n+x} E_n(x). \tag{11.4.7}$$

Assume there is a function $f(x)$ defined by $f(x) = \lim_{n\to\infty} E_n(x)$. Then, if the convergence is such that derivatives and limits can be exchanged, the limiting function f satisfies $f'(x) = f(x)$. Conclude that $f(x) = \exp(x)$.

Exercise 11.4.6. Define

$$F_n(x) := \sum_{j=0}^{n} \frac{x^j}{j!}. \tag{11.4.8}$$

Prove that $F_n'(x) = F_{n-1}(x)$. Establish the inequality $F_n(x) \leq e^x$ for $x \geq 0$. Conclude that e^x is an increasing function satisfying

$$\lim_{x\to\infty} e^x = \infty.$$

Define

$$G_n(x) = F_n(x)F_n(-x). \tag{11.4.9}$$

Prove that

$$G_n(x) = 1 + \frac{(-1)^n}{n!^2} K_n(x),$$

where K_n is a polynomial with positive integer coefficients of degree $n+2$ for n even and $n+1$ if n is odd. Explore properties of the polynomial K_n.

11.5. Arithmetical properties of e

This section discusses properties of e that have somewhat of an arithmetic nature. The first result establishes the irrationality of e. This was shown by J. H. Lambert in 1761 [**191**]. C. Hermite [**167**] proved that e is **transcendental**, that is, e is not the root of a polynomial with integer coefficients. The reader will find a proof of this result in the text by G. H. Hardy et al. [**160**]. This section also includes a result of J. Liouville [**200**] and S. Beatty [**45**] that neither e nor e^2 satisfies a polynomial equation of degree 2.

Theorem 11.5.1. *The number e is irrational.*

First proof. Assume $e \in \mathbb{Q}$ and write it as $e = m/n$, with $m,\, n \in \mathbb{N}$. The previous section has provided estimates on the partial sums e_n in the form

$$0 < e - e_n < \frac{1}{n\, n!}. \tag{11.5.1}$$

This yields

$$0 < (n-1)!m - n!e_n < \frac{1}{n} < 1. \tag{11.5.2}$$

This is a contradiction because the middle term is an integer.

A geometric proof. This proof is due to J. Sondow [**275**]. Exercise 11.3.3 shows that $e \in I_1 := [2,\, 3]$. Divide this interval in two equal parts and let I_2 be the second one, that is, $I_2 = [\frac{5}{2},\, 3]$. The estimate

$$e > 1 + 1 + \frac{1}{2!} = \frac{5}{2} = e_2 \tag{11.5.3}$$

shows that $e \in I_2$. Proceed by induction and divide I_{k-1} into k equal subintervals and let I_k be the second one. Then

$$I_k = [e_k, e_k + \tfrac{1}{k!}] \tag{11.5.4}$$

and $e \in I_k$ because $e > e_k$. Then

$$e = \bigcap_{k=1}^{\infty} I_k \tag{11.5.5}$$

is the geometric equivalent of the series representation (11.4.3). This proves that if e is rational, say $\frac{m}{n}$, then n cannot be of the form $k!$.

But every fraction can be written with a factorial as denominator, as in

$$\frac{m}{n} = \frac{m \cdot (n-1)!}{n!}. \tag{11.5.6}$$

This contradicts the assumption that e is rational.

A third proof based on continued fractions is presented in Corollary 11.6.9.

11.5.1. Quadratic irrationality of e. Suppose that e satisfies $ae^2 + be + c = 0$, with a, b, $c \in \mathbb{Z}$ and $a \neq 0$. The series representation of e gives

$$n!e = \sum_{k=0}^{n} \frac{n!}{k!} + \sum_{k=n+1}^{\infty} \frac{n!}{k!}.$$

The second term is bounded by

$$\sum_{k=n+1}^{\infty} \frac{n!}{k!} > \frac{n!}{(n+1)!} = \frac{1}{n+1} \tag{11.5.7}$$

and

$$\sum_{k=n+1}^{\infty} \frac{n!}{k!} < \sum_{j=1}^{\infty} \frac{1}{(n+1)^j} = \frac{1}{n}. \tag{11.5.8}$$

It follows that

$$\sum_{k=n+1}^{\infty} \frac{n!}{k!} = \frac{1}{n+t} \tag{11.5.9}$$

with $0 < t < 1$. The value of t naturally depends upon n. A similar argument shows that

$$\sum_{k=n+1}^{\infty} (-1)^k \frac{n!}{k!} = \frac{(-1)^{n+1}}{n+1+s}, \tag{11.5.10}$$

with $0 < s < 1$, which depends upon n. Multiply the quadratic equation satisfied by e by $n!/e$ to obtain

$$a\left(i + \frac{1}{n+t}\right) + bn! + c\left(j + \frac{(-1)^{n+1}}{n+1+s}\right) = 0, \tag{11.5.11}$$

for some integers i, j. This yields

$$\frac{a}{n+t} + \frac{c}{n+1+s} = -(ai + bn! + cj). \tag{11.5.12}$$

The right-hand side is an integer and the left-hand side is arbitrarily small for large n. It follows that $a = -c$ and $t - s = 1$. This is impossible and proves the next theorem, due to J. Liouville.

Theorem 11.5.2. *There is no nonzero polynomial $P(x) = ax^2 + bx + c$, with a, b, $c \in \mathbb{Z}$, such that $P(e) = 0$.*

11.5.2. Quadratic irrationality of e^2. The next step is to prove a similar result for e^2.

Theorem 11.5.3. *There is no nonzero polynomial $P(x) = ax^4 + bx^2 + c$, with a, b, $c \in \mathbb{Z}$, such that $P(e) = 0$.*

Proof. Legendre's theorem, Theorem 2.6.4, shows that the 2-adic valuation of $n!$ is given by

$$\nu_2(n!) = n - s_2(n), \tag{11.5.13}$$

where $s_2(n)$ is the sum of the binary digits of n. Now write

$$\frac{2^n}{n!} = \frac{2^{s_2(n)}}{\mathcal{O}_n}, \tag{11.5.14}$$

with $\mathcal{O}_n$ an odd number. Observe that $\mathcal{O}_n$ is the **odd part** of $n!$, obtained by removing all factors of 2 from $n!$. Therefore, if $n > m$, then $\mathcal{O}_m$ divides $\mathcal{O}_n$. Now assume that $ae^4 + be^2 + c = 0$ for some integers a, b, c, where a may be assumed to be positive. The equation becomes

$$ae^2 + ce^{-2} = -b. \tag{11.5.15}$$

The Taylor expansion of the exponential is given by

$$e^x = 1 + x + \frac{x^2}{2!} + \cdots + \frac{x^n}{n!}\left(1 + \frac{x}{n+1}e^{x\,\theta(x)}\right),$$

where $0 < \theta(x) < 1$. For each $n \in \mathbb{N}$, define

$$\beta_n = \frac{e^{2\theta(2)}}{n+1} \quad \text{and} \quad \gamma_n = \frac{e^{-2\theta(-2)}}{n+1}. \tag{11.5.16}$$

Therefore

$$e^2 = 1 + 2 + \frac{2^2}{2!} + \cdots + \frac{2^n}{n!}(1 + 2\beta_n)$$

and

$$e^{-2} = 1 - 2 + \frac{2^2}{2!} - \cdots \pm \frac{2^n}{n!}(1 - 2\gamma_n),$$

where the $+$ sign appears if n is even and the $-$ sign appears if n is odd.

The equation (11.5.15) becomes

$$a\left(1+2+\frac{2^2}{2!}+\cdots+\frac{2^n}{n!}(1+2\beta_n)\right)$$
$$+\,c\left(1-2+\frac{2^2}{2!}-\cdots\pm\frac{2^n}{n!}(1-2\gamma_n)\right)=-b.$$

Exercise 11.5.4. Prove that

$$2^{\alpha_n+1}a\beta_n \mp 2^{\alpha_n+1}c\gamma_n = d, \tag{11.5.17}$$

where d is an integer and $a>0$.

If $c \neq 0$, choose the integer n so that $\mp c > 0$. For example, if $c>0$, take $n=2^i+1$. This means that in the expansion of e^{-2}, a minus sign appears at the last term.

Exercise 11.5.5. Prove that the above choices imply $\alpha_n = 1$ and (11.5.17) becomes

$$4a\beta_n + 4(-c)\gamma_n = d. \tag{11.5.18}$$

This is a contradiction. The left-hand side of (11.5.18) is positive and it lies strictly between 0 and 1 by choice of $n=2^i+1$ large enough. A similar contradiction appears if $c<0$, this time choosing $n=2^i$. The final case of $c=0$ is elementary and it is left to the reader. □

Note 11.5.6. C. Hermite proved that there is no polynomial P with integer coefficients such that $P(e)=0$; that is, e is transcendental. An outline of the proof may be found as Exercise 4, Section 11.2, page 353 of the book by J. M. and P. B. Borwein [**71**]. The proof presented next appears in the class notes by M. Filaseta [**126**].

Theorem 11.5.7. *The number e is transcendental.*

Proof. The proof is divided into a small number of steps.

Step 1. Let f be a polynomial of degree n. Define

$$I(t)=\int_0^t e^{t-u}f(u)\,du.$$

Exercise 11.5.8. Prove that

$$I(t) = e^t \sum_{j=0}^{n} f^{(j)}(0) - \sum_{j=0}^{n} f^{(j)}(t).$$

Hint: Integrate by parts.

Exercise 11.5.9. For a polynomial $f(x) = a_0 + a_1 x + \cdots + a_n x^n$, define $f^*(x) = |a_0| + |a_1|x + \cdots + |a_n|x^n$. Prove that

$$|I(t)| \leq |t| f^*(|t|) e^{|t|}.$$

Step 2. Assume $g(x) = b_0 + b_1 x + \cdots + b_r x^r$ is a polynomial, with $b_j \in \mathbb{Z}$ and $b_0 \neq 0$, such that $g(e) = 0$. Define

$$f(x) = x^{p-1}(x-1)^p(x-2)^p \cdots (x-r)^p$$

and form the expression

$$J = b_0 I(0) + b_1 I(1) + \cdots + b_r I(r),$$

where $I(t)$ is computed with the polynomial f. Observe that the degree of f is $n = (r+1)p - 1$. Then

$$\begin{aligned} J &= \sum_{k=0}^{r} b_k I(k) = \sum_{k=0}^{r} b_k \left(e^k \sum_{j=0}^{n} f^{(j)}(0) - \sum_{j=0}^{n} f^{(j)}(k) \right) \\ &= \left(\sum_{j=0}^{n} f^{(j)}(0) \right) g(e) - \sum_{k=0}^{r} \sum_{j=0}^{n} b_k f^{(j)}(k) \\ &= -\sum_{k=0}^{r} \sum_{j=0}^{n} b_k f^{(j)}(k). \end{aligned}$$

The polynomial f has a zero of order $p-1$ at $x = 0$; therefore $f^{(j)}(0) = 0$ for $0 \leq j \leq p-2$. Similarly, $f^{(j)}(k) = 0$ for $0 \leq j \leq p-1$. This gives

$$J = -b_0 f^{(p-1)}(0) - b_0 \sum_{j=p}^{n} f^{(j)}(0) + \sum_{k=1}^{r} b_k \sum_{j=p}^{n} f^{(j)}(k). \tag{11.5.19}$$

Exercise 11.5.10. Check that

$$\left(\frac{d}{dx}\right)^s x^{p-1}\Big|_{x=0} = \begin{cases} (p-1)! & \text{if } s = p-1, \\ 0 & \text{if } s \neq p-1. \end{cases}$$

Step 3. Assume $p > \text{Max}\{|b_0|, r\}$. Then every term in (11.5.19), except the first one, is divisible by $p!$. To verify this claim, first take $j \geq p$ and write

$$f(x) = x^{p-1}h(x). \tag{11.5.20}$$

Differentiation now gives

$$\begin{aligned} f^{(j)}(0) &= \sum_{s=0}^{j} \binom{j}{s} \left(\frac{d}{dx}\right)^s x^{p-1}\Big|_{x=0} \cdot \left(\frac{d}{dx}\right)^{j-s} h(x)\Big|_{x=0} \\ &= \binom{j}{p-1} \cdot (p-1)! \left(\frac{d}{dx}\right)^{j-p+1} h(x)\Big|_{x=0}, \end{aligned}$$

with the result

$$f^{(j)}(0) = j(j-1)(j-2)\cdots(j-p+2) \cdot \left(\frac{d}{dx}\right)^{j-p+1} h(x)\Big|_{x=0}.$$

The first term is the product of $p-1$ consecutive integers. Corollary 2.1.7 shows that this number is divisible by $(p-1)!$. Every derivative of the second term is a sum where the terms contain at least one derivative of the factors $(x-k)^p$. Therefore, this term is divisible by p.

Exercise 11.5.11. Check that, for $j \geq p$ and $1 \leq k \leq r$, the number $p!$ divides $f^{(j)}(k)$.

Finally,

$$f^{(p-1)}(0) = (-1)^{rp}(p-1)! \cdot (r!)^p$$

is not divisible by $p!$ because $r < p$.

Step 4. The number J is divisible by $(p-1)!$ and $J \neq 0$ since J is not divisible by $p!$. Therefore $|J| \geq (p-1)!$. The bounds for J shown in Exercise 11.5.8 give

$$|J| \leq \sum_{k=0}^{r} |b_k| k f^*(k) e^k. \tag{11.5.21}$$

For $0 \leq k \leq r$,

$$f^*(k) = k^{p-1}(k+1)^p(k+2)^p \cdots (k+r)^p \leq r^{p-1}(2r)^{rp} \leq (2r)^{(r+1)p}.$$

This yields $|J| \leq ca^p$, with $a = (2r)^{r+1}$ and c constants independent of p. The inequalities

$$(p-1)! \leq |J| \leq ca^p \tag{11.5.22}$$

are incompatible for large p. The proof is complete. □

11.6. Continued fractions connected to e

Continued fractions were introduced in Chapter 1 in the context of the Euclidean algorithm. This was extended to real numbers in Subsection 1.9.5. In this section a number of continued fractions that produce expressions related to e are discussed.

Theorem 11.6.1. *The continued fraction for e is given by*

$$e = [2, 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, 8, 1, \ldots]. \tag{11.6.1}$$

The proof presented here appears in the text by J. Roberts [**255**].

Step 1. Introduce the function

$$f_n(x) = \sum_{j=0}^{\infty} a_{n,j} x^{2j} \quad \text{where } a_{n,j} = \frac{(n+j)!}{j!\,(2n+2j)!}.$$

Exercise 11.6.2. Prove that the series converges for all $x \in \mathbb{R}$.

Step 2. The series $f_n(x)$ satisfies the recurrence

$$f_n(x) = 2(2n+1)f_{n+1}(x) = 4x^2 f_{n+2}(x).$$

Proof. A direct calculation shows that

$$a_{n,j} - 2(2n+1)a_{n+1,j} = \frac{2(n+j)!}{(j-1)!\,(2n+2j+1)!}.$$

Multiply by x^{2j} and sum for $j \geq 1$. This yields

$$\begin{aligned}\sum_{j=1}^{\infty} a_{n,j}x^{2j} - \sum_{j=1}^{\infty} 2(2n+1)a_{n+1,j}x^{2j} &= 2\sum_{j=1}^{\infty} \frac{(n+j)!x^{2j}}{(j-1)!(2n+2j+1)!} \\ &= 2x^2 \sum_{j=0}^{\infty} \frac{(n+j+1)!x^{2j}}{j!(2n+2j+3)!} \\ &= 4x^2 \sum_{j=0}^{\infty} \frac{(n+j+2)!}{j!(2n+2j+4)!} x^{2j}.\end{aligned}$$

This is the claim.

Step 3. The initial terms for the sequence $f_n(x)$ are

$$f_0(x) = \frac{e^x + e^{-x}}{2} \quad \text{and} \quad f_1(x) = \frac{1}{2x} \cdot \frac{e^x - e^{-x}}{2}.$$

Proof. A direct calculation shows that

$$f_0(x) = \sum_{j=0}^{\infty} \frac{x^{2j}}{(2j)!} = \frac{e^x + e^{-x}}{2}$$

and similarly for $f_1(x)$.

Step 4. Introduce the quotient

$$g_n(x) = \frac{f_n(x)}{f_{n+1}(x)} \tag{11.6.2}$$

and write the recurrence in Step 2 in the form

$$g_n(x) = 4n + 2 + \frac{1}{\frac{1}{4x^2} \cdot g_{n+1}(x)}. \tag{11.6.3}$$

Observe that

$$\frac{e^{2x}+1}{e^{2x}-1} = \frac{1}{2x} g_0(x) \tag{11.6.4}$$

and the recurrence (11.6.3) gives

$$g_0(x) = 2 + \frac{1}{\frac{1}{4x^2} \cdot g_1(x)}. \tag{11.6.5}$$

This leads to

$$\frac{e^{2x}+1}{e^{2x}-1} = \frac{1}{x} + \frac{1}{\frac{1}{2x} \cdot g_1(x)}. \tag{11.6.6}$$

Exercise 11.6.3. Check that iterating the previous procedure gives the continued fraction

$$\frac{e^{2x}+1}{e^{2x}-1} = \left[\frac{1}{x}, \frac{3}{x}, \frac{5}{x}, \ldots, \frac{2n-1}{x}, \frac{2n+1}{x} + \frac{2x}{g_{n+1}(x)} \right]. \tag{11.6.7}$$

The Seidel-Stern theorem stated next guarantees that the limit as $n \to \infty$ exists. The reader will find a proof in the book by L. Lorentzen and H. Waadeland [**204**].

Theorem 11.6.4. *Let $a_0 \in \mathbb{R}$ and $a_j \in \mathbb{R}^+$ for $j \geq 1$. The continued fraction $[a_0, a_1, \ldots, a_n]$ has a limit as $n \to \infty$ if and only if $\sum_n a_n$ diverges.*

Theorem 11.6.5. *The continued fraction*

$$\frac{e^{2x}+1}{e^{2x}-1} = \left[\frac{1}{x}, \frac{3}{x}, \frac{5}{x}, \ldots, \frac{2n-1}{x}, \ldots \right] \tag{11.6.8}$$

holds for all $x \in \mathbb{R}$.

Example 11.6.6. The choice $x = \frac{1}{2}$ gives

$$\frac{e+1}{e-1} = [2,\, 6,\, 10,\, 14, \ldots].$$

This continued fraction, also written as

$$\frac{e+1}{e-1} = 2 + \cfrac{1}{1 + \cfrac{6}{1 + \cfrac{10}{1 + \cfrac{14}{1 + \cfrac{18}{\cdots}}}}},$$

was discovered by Euler in 1737.

The last step in the proof of Theorem 11.6.1 is to prove that if

$$\alpha = [a_0,\, a_1,\, a_2,\, \ldots] \tag{11.6.9}$$

where

$$a_0 = 2, \quad a_{3n} = a_{3n+1} = 1, \quad a_{3n-1} = 2n, \tag{11.6.10}$$

then $\alpha = e$. This is accomplished by comparing the convergents of α and those of $(e-1)/(e+1)$.

The next exercise can be checked by induction using the rules for convergents in Exercise 1.9.22.

Exercise 11.6.7. Let $\dfrac{p_n}{q_n}$ be the convergents of α and let $\dfrac{u_n}{v_n}$ be the convergents of $\dfrac{e+1}{e-1}$.

(a) The relations

$$\begin{aligned} p_{3n+1} &= 2(2n+1)p_{3n-2}+p_{3n-5} \quad \text{for } n \geq 2, \\ q_{3n+1} &= 2(2n+1)q_{3n-2}+q_{3n-5} \quad \text{for } n \geq 1 \end{aligned}$$

hold.

(b) The convergents of α and $\dfrac{e+1}{e-1}$ are related by

$$\begin{aligned} 2u_n &= p_{3n+1}+q_{3n+1}, \\ 2v_n &= p_{3n+1}-q_{3n+1}. \end{aligned}$$

The next exercise completes the proof of Theorem 11.6.1.

Exercise 11.6.8. Use the relation

$$\frac{p_{3n+1}+q_{3n+1}}{p_{3n+1}-q_{3n+1}} = \frac{u_n}{v_n} \tag{11.6.11}$$

to conclude that $\alpha = e$. **Hint:** First check that $\alpha \neq 1$ and then pass to the limit in (11.6.11).

Corollary 11.6.9. *The number e is irrational.*

Proof. Example 11.6.6 shows that the number $(e+1)/(e-1)$ is irrational since the continued fraction appearing there is not finite. This implies the result. □

Exercise 11.6.10. A very nice proof of the continued fraction for e was given by H. Cohn [**103**]. This proof is outlined in a number of steps. Check the details.

(1) The continued fraction

$$e = [2,1,2,1,1,4,1,1,6,1,1,8,1,1,10,\ldots]$$

may be written as $e = [1,0,1,1,2,1,1,4,1,1,6,1,1,8,1,1,10,\ldots]$. Write the terms of the continued fraction as $e = [a_0,a_1,a_2,\ldots]$.

(2) Use the rules in Exercise 1.9.22 to check that the convergents $[a_0, a_1, \ldots, a_i] = p_i/q_i$ satisfy

$$p_{3n} = p_{3n-1} + p_{3n-2},\ p_{3n+1} = 2np_{3n} + p_{3n-1},\ p_{3n+2} = p_{3n+1} + p_{3n},$$

and the same rules holds for q_i.

(3) Define the integrals

$$\begin{aligned} A_n &= \int_0^1 \frac{x^n(x-1)^n}{n!} e^x\, dx, \\ B_n &= \int_0^1 \frac{x^{n+1}(x-1)^n}{n!} e^x\, dx, \\ C_n &= \int_0^1 \frac{x^n(x-1)^{n+1}}{n!} e^x\, dx. \end{aligned}$$

Integrate by parts to check the relations

$$A_n = -B_{n-1} - C_{n-1}, \quad B_n = -2nA_n + C_{n-1}, \quad C_n = B_n - A_n.$$

(4) Use the relations in (3) to prove that

$$A_n = eq_{3n} - p_{3n}, \quad B_n = p_{3n+1} - eq_{3n+1}, \quad C_n = p_{3n+2} - eq_{3n+2}.$$

Conclude that $p_i/q_i \to e$.

11.7. Derangements: The presence of e in combinatorics

An interesting appearance of the constant e is in a special counting problem. Consider a permutation π of the n numbers $\{1, 2, \ldots, n\}$. The number i is said to be **fixed** by π if $\pi(i) = i$.

Definition 11.7.1. A permutation π of $\{1, 2, \ldots, n\}$ without any fixed point is called a **derangement**. The number of derangements is denoted by D_n. The first few values are 1, 0, 1, 2, 9, 44.

Note 11.7.2. This notion used to be explained in terms of gentlemen arriving at a party and placing their hats on a table. At the moment of departure, each of them takes a hat at random. The derangement counts the chance of nobody taking the correct hat. These days, hats are not in fashion, so this interpretation is no longer employed.

A closed-form formula for D_n is now derived using the ***inclusion-exclusion principle*** described in Theorem 7.3.1. To produce an expression for the derangement number, for each i in the range $1 \leq i \leq n$, let

$$A_i = \{\pi \in S_n : \pi(i) = i\} \tag{11.7.1}$$

be the set of permutations in the symmetric group S_n that fix i. Then

$$D_n = \left| \bigcap_{i=1}^{n} A_i^c \right| = n! - \left| \bigcup_{i=1}^{n} A_i \right|. \tag{11.7.2}$$

The number

$$|A_{i_1} \cap A_{i_2} \cap \cdots \cap A_{i_k}| \tag{11.7.3}$$

is needed to apply the inclusion-exclusion principle. A permutation in this set fixes k indices and permutes the remaining $n-k$. Therefore

$$|A_{i_1} \cap A_{i_2} \cap \cdots \cap A_{i_k}| = (n-k)!$$

and it follows that

$$\left| \bigcup_{i=1}^{n} A_i \right| = n \times (n-1)! - \binom{n}{2} \times (n-2)! + \binom{n}{3} \times (n-3)! - \cdots .$$

This provides the expression for the derangement number stated next.

Theorem 11.7.3. *The derangement number is given by*

$$D_n = n! \times \sum_{k=0}^{n} \frac{(-1)^k}{k!}. \tag{11.7.4}$$

Passing to the limit as $n \to \infty$ makes the number $1/e$ appear.

Corollary 11.7.4. *As $n \to \infty$, the proportion of permutations of n elements that do not have a fixed point is given by*

$$\lim_{n\to\infty} \frac{D_n}{n!} = \frac{1}{e}. \tag{11.7.5}$$

The next series of exercises discusses some properties of the derangement numbers D_n.

Exercise 11.7.5. Establish the recurrence

$$D_n = (n-1)\left(D_{n-1} + D_{n-2}\right). \tag{11.7.6}$$

Hint: Let π be a permutation without fixed points. Assume $\pi(1) = 2$ and divide these permutations into two types according to whether $\pi(2) = 1$ or not.

Exercise 11.7.6. Write the recurrence in Exercise 11.7.5 in the form

$$D_n - nD_{n-1} = -\left[D_{n-1} - (n-1)D_{n-2}\right].$$

Iterate to produce

$$D_n = nD_{n-1} + (-1)^n. \tag{11.7.7}$$

Exercise 11.7.7. Use (11.7.7) to produce the generating function

$$\sum_{n=0}^{\infty} \frac{D_n}{n!} x^n = \frac{e^{-x}}{1-x}. \tag{11.7.8}$$

Exercise 11.7.8. Prove that D_n is the nearest integer to $n!/e$.

Exercise 11.7.9. The recurrence in Exercise 11.7.5 shows that $n-1$ divides D_n. Define

$$D_n^* = \frac{D_n}{n-1}. \tag{11.7.9}$$

Prove that

$$D_n^* = n(n-3)D_{n-2}^* + (-1)^{n-1} \tag{11.7.10}$$

and conclude that D_n^* is an odd integer.

Exercise 11.7.10. Let $r \in \mathbb{N}$ and let D_n^* be as in Exercise 11.7.9. Prove that the sequence D_n^* mod r is periodic and that its minimal period is r if r is even and $2r$ if r is odd. Compare this with the similar question for Fibonacci numbers described in Section 3.6.

Note 11.7.11. An attempt to study the factorization of D_n^* showed that this number sometimes is prime. The set of indices $n \leq 5000$ for which this occurs is

$$\{4,\ 5,\ 6,\ 11,\ 15,\ 44,\ 66,\ 168,\ 575,\ 1713\}.$$

These numbers do not appear in N. Sloane's database. The prime numbers appearing in this list grow very rapidly. The number of digits of the entries in the previous list is given by

$$\{1,\ 2,\ 2,\ 7,\ 11,\ 53,\ 91,\ 300,\ 1336,\ 4794\}.$$

Exercise 11.7.12. This problem comes from Benoit Cloitre's website

`http://www.pi314.net/eng/miroir.php`

and it is complemented by Exercise 12.6.5. Define

$$u_n = u_{n-1} + \frac{1}{n-2} u_{n-2} \tag{11.7.11}$$

for $n \geq 3$ and $u_1 = 0$, $u_2 = 1$. Prove that the generating function

$$U(x) = \sum_{n=1}^{\infty} u_n x^n \tag{11.7.12}$$

satisfies

$$x(x-1)U'(x) + (x^2 - x + 2)U(x) = 0. \tag{11.7.13}$$

Integrate to produce

$$U(x) = \frac{x^2 e^{-x}}{(1-x)^2}. \tag{11.7.14}$$

Verify the identity

$$U(x) = x \frac{d}{dx} \left(\frac{e^{-x}}{1-x} \right) \tag{11.7.15}$$

and use it to produce

$$u_n = n \sum_{j=0}^{n} \frac{(-1)^j}{j!} = \frac{D_n}{(n-1)!}. \tag{11.7.16}$$

Conclude that

$$\lim_{n \to \infty} \frac{n}{u_n} = e. \tag{11.7.17}$$

Note 11.7.13. A simple calculation gives the integral representation

$$D_n = \int_0^{\infty} (t-1)^n e^{-t} \, dt. \tag{11.7.18}$$

This note contains a description of the beautiful explanation of this identity given in the paper by P. M. Kayll [**182**].

The description starts with a graph $G = (V, E)$ formed by a collection of vertices V and a collection of edges E. Each edge $e \in E$ connects two vertices in V. The graph G is called **bipartite** if the vertices V are divided into two disjoint sets $V = X \cup Y$ in such a way that each edge connects a vertex from X to one from Y. A **matching** of G is a collection of edges $M \subset E$ such that the edges in M do not share vertices. If every vertex is part of some edge in M, then M is called a **perfect matching**.

Exercise 11.7.14. Prove that if G has a perfect matching, then $|X| = |Y|$. Conclude that G contains all the vertices of the **complete bipartite** graph $K_{n,n}$. This is a bipartite graph with vertex set $V = X \cup Y$ with every vertex in X connected to every vertex in Y. The graph G is called a **spanning subgraph** of $K_{n,n}$.

For a graph G, let $\mu_G(r)$ be the number of matchings in G containing exactly r edges. Assume G is the spanning subgraph of $K_{n,n}$. The **rook polynomial** of G is defined by

$$R_G(t) = \sum_{r=0}^{n} (-1)^r \mu_G(r) t^{n-r}. \tag{11.7.19}$$

Exercise 11.7.15. Let G be a graph with n pairwise disjoint vertices. Prove that $\mu_G(r) = \binom{n}{r}$. Conclude that $R_G(t) = (t-1)^n$.

For a bipartite graph G, let $\Xi(G)$ denote the number of perfect matchings of G and let $G^{\sim}$ be the **bipartite complement** of G: this is the graph with the same vertices as G and has for edges all the edges in the complete bipartite graph $K_{n,n}$ that are not in G. The next theorem relates these concepts. The reader will find the required background in the textbook by J. Riordan [**253**].

Theorem 11.7.16. *If H is a spanning subgraph of $K_{n,n}$, then*

$$\Xi(H) = \int_0^\infty e^{-t} R_{H^{\sim}}(t)\, dt. \tag{11.7.20}$$

Exercise 11.7.17. Let G be the graph obtained by removing from $K_{n,n}$ the edges of a perfect matching. Check that every perfect matching of G corresponds to a derangement of $\{1, 2, \ldots, n\}$.

The integral expression (11.7.18) now follows from Theorem 11.7.16 and Exercise 11.7.15. For more examples and a description of the relations between integrals and other combinatorial objects, the reader is referred to [**182**].

11.8. The natural logarithm

The exponential function e^x is an increasing function that maps $\mathbb{R}$ to $(0, \infty)$. The **natural logarithm** is defined as its inverse. The notation $\ln x$ is employed. The basic properties are derived from the inverse function theorem stated next.

Theorem 11.8.1. *Let f be continuous on $[a, b]$, differentiable on (a, b), and suppose $f'(x) \neq 0$ on (a, b). Let $[m, M] = f([a, b])$. Then, $f : [a, b] \to [m, M]$ is invertible and its inverse g is continuous on $[m, M]$, differentiable on (m, M), and $g'(y) \neq 0$ on (m, M). Moreover,*

$$g'(y) = \frac{1}{f'(g(y))}, \quad m < y < M. \tag{11.8.1}$$

The reader will find in the textbook by O. Hijab [**168**] a readable proof.

Exercise 11.8.2. Prove the integral representation

$$\ln x = \int_1^x \frac{dt}{t}. \tag{11.8.2}$$

Exercise 11.8.3. The functional equation

$$\ln(xy) = \ln x + \ln y \tag{11.8.3}$$

for x, $y \in \mathbb{R}^+$ follows directly from Theorem 11.2.1. Give a direct proof from the integral representation (11.8.2). **Hint:** Split the integral over $[1, xy]$ at x.

Theorem 11.8.4. *The power series expansion of $y = \ln(1 - x)$ for $|x| < 1$ is given by*

$$\ln(1 - x) = -\sum_{k=1}^{\infty} \frac{x^k}{k}. \tag{11.8.4}$$

Proof. Integrate the geometric series $\dfrac{1}{1-x} = 1 + x + x^2 + \cdots$. □

Exercise 11.8.5. Prove the expansion

$$\ln \frac{1+x}{1-x} = 2\sum_{k=0}^{\infty} \frac{x^{2k+1}}{2k+1}. \tag{11.8.5}$$

This is valid for $|x| < 1$.

As in the case of the exponential function, it is relatively simple to establish that $\ln x$ is not a rational function.

Theorem 11.8.6. *There is no rational function $R(x)$ such that*

$$R'(x) = \frac{1}{x}.$$

That is, $y = \ln x$ is not a rational function.

Proof. Let $R(x) = B(x)/A(x)$ (with $\gcd(A,B) = 1$) and assume $R'(x) = 1/x$. This yields

$$x(B'(x)A(x) - B(x)A'(x)) = A^2(x). \tag{11.8.6}$$

This shows that $x = 0$ is a root of A. Write $A(x) = x^r C(x)$, with $C(0) \neq 0$ and $r > 0$. Then (11.8.6) produces

$$xB'(x)C(x) - B(x)\left[rC(x) + xC'(x)\right] = x^r C^2(x). \tag{11.8.7}$$

Let $x = 0$ to obtain $rB(0)C(0) = 0$. This is a contradiction. □

11.9. The binary expansion of $\ln 2$

The value $x = \frac{1}{2}$ in (11.8.4) yields

$$\ln 2 = \sum_{k=1}^{\infty} \frac{1}{k2^k}, \tag{11.9.1}$$

which has been known at least since the time of Euler. For any $d \in \mathbb{N}$, the series (11.8.5) implies

$$2^d \ln 2 = \sum_{k=1}^{d} \frac{2^{d-k}}{k} + \sum_{k=d+1}^{\infty} \frac{2^{d-k}}{k}. \tag{11.9.2}$$

The next exercise appears in the paper by D. H. Bailey, P. Borwein, and S. Plouffe [**37**], and it was a precursor of the so-called BBP-formulas. See Section 12.8 for a similar formula for π.

Exercise 11.9.1. Use the binary expansion of the integer n to provide an algorithm that evaluates a^n in an efficient manner. The example

$$5^{17} = ((((5^2)^2)^2)^2) \cdot 5 \tag{11.9.3}$$

should provide a hint.

Exercise 11.9.2. Let r mod 1 be the fractional part of the real number r and let x mod k be the residue of the integer x modulo k. Prove that

$$\begin{aligned}\left(2^d \ln 2\right) \text{ mod } 1 &= \left(\sum_{k=1}^{d} \frac{2^{d-k}}{k} \text{ mod } 1 + \sum_{k=d+1}^{\infty} \frac{2^{d-k}}{k} \text{ mod } 1 \right) \text{ mod } 1. \\ &= \left(\sum_{k=1}^{d} \frac{2^{d-k} \text{ mod } k}{k} \text{ mod } 1 + \sum_{k=d+1}^{\infty} \frac{2^{d-k}}{k} \text{ mod } 1 \right) \text{ mod } 1.\end{aligned}$$

Discuss how to employ this formula to evaluate the binary digits of $\ln 2$. The evaluation of 2^{d-k} in the first sum can be done using Exercise 11.9.1.

11.10. The irrationality of ln 2

This section is based on work presented in the book by J. M. and P. B. Borwein [**71**] and in the paper by D. Huylebrouck [**177**].

The main result required in the proof is an estimate on the growth of the least common multiple of the first n integers. The first theorem shows that this estimate implies the irrationality of $\ln 2$. The remainder of the section presents an elementary proof of this estimate. A much shorter argument, based on the prime number theorem, is outlined at the end of the section.

Theorem 11.10.1. *Define*

$$d_n = \text{lcm}\{1,\, 2,\, ,\ldots, n\}. \tag{11.10.1}$$

Then $d_n \leq 3^n$.

The proof of this theorem is presented at this end of this section.

Theorem 11.10.2. *Theorem* 11.10.1 *implies that* $\ln 2$ *is irrational.*

Proof. Assume that $\ln 2 = \dfrac{a}{b}$ with a, $b \in \mathbb{N}$. The first part of the proof consists of finding an integral that produces $\ln 2$. Integrating the identity

$$\frac{x^n}{1+x} = \frac{x^n - (-1)^n}{x+1} + \frac{(-1)^n}{x+1}$$

shows that

$$\int_0^1 \frac{x^n\,dx}{1+x} = \frac{u_n + v_n \ln 2}{d_n} \tag{11.10.2}$$

where u_n, $v_n \in \mathbb{Z}$.

Define

$$f_n(x) = \frac{1}{n!}\left(\frac{d}{dx}\right)^n x^n(1-x)^n. \tag{11.10.3}$$

Exercise 11.10.3. Prove that f_n is a polynomial with integer coefficients.

Let

$$I_n = \int_0^1 f_n(x)\frac{dx}{1+x}. \tag{11.10.4}$$

Then there are integers u_n^*, v_n^* such that

$$I_n = \frac{u_n^* + v_n^* \ln 2}{d_n}. \tag{11.10.5}$$

Integration by parts shows that

$$I_n = \int_0^1 \left[\frac{x(1-x)}{1+x}\right]^n \frac{dx}{1+x}.$$

The estimate

$$\frac{x(1-x)}{1+x} \leq 3 - 2\sqrt{2} \tag{11.10.6}$$

and Theorem 11.10.1 give

$$0 < |u_n^* + v_n^* \ln 2| = I_n d_n \leq (3-2\sqrt{2})^n d_n \leq (9-6\sqrt{2})^n.$$

The inequality $9 - 6\sqrt{2} < 1$ shows that $(9 - 6\sqrt{2})^n < 1/b$ for n sufficiently large. This produces

$$0 < |bu_n^* + av_n^*| < 1. \tag{11.10.7}$$

This is a contradiction. □

11.10.1. Bounds on $\text{lcm}(1, 2, \ldots, n)$**.** The goal of this subsection is to present D. Hanson's proof [**157**] of Theorem 11.10.1. The proof is divided into a sequence of steps.

Step 1. The least common multiple is given by

$$d_n = \prod_{p \leq n} p^{\alpha_p(n)} \tag{11.10.8}$$

where

$$\alpha_p(n) = \left\lfloor \frac{\ln n}{\ln p} \right\rfloor \tag{11.10.9}$$

is the highest power of p below n.

Exercise 11.10.4. Let $u \in \mathbb{R}$ and $m \in \mathbb{N}$. Prove that

$$\left\lfloor \frac{u}{m} \right\rfloor = \left\lfloor \frac{\lfloor u \rfloor}{m} \right\rfloor.$$

Step 2. Let x_1, $x_2, \ldots, x_k$ be positive integers satisfying

$$\sum_{j=1}^{k} \frac{1}{x_j} \leq 1.$$

If $x \in \mathbb{R}$ is such that $x_k > x \geq 1$, then

$$\lfloor x \rfloor > \sum_{j=1}^{k} \left\lfloor \frac{x}{x_j} \right\rfloor.$$

Proof. Using Exercise 11.10.4,

$$\begin{aligned} \sum_{j=1}^{k} \left\lfloor \frac{x}{x_j} \right\rfloor &= \sum_{j=1}^{k-1} \left\lfloor \frac{x}{x_j} \right\rfloor = \sum_{j=1}^{k-1} \left\lfloor \frac{\lfloor x \rfloor}{x_j} \right\rfloor \\ &\leq \sum_{j=1}^{k-1} \frac{\lfloor x \rfloor}{x_j} \leq \lfloor x \rfloor \left(1 - \frac{1}{x_k} \right) < \lfloor x \rfloor \end{aligned}$$

and the result has been established. □

Exercise 11.10.5. This exercise is related to the sequence discussed in Lemma 1.7.9. Choose $a_1 = 2$ and $a_{n+1} = a_1 a_2 \cdots a_n + 1$. Prove that $a_{n+1} = a_n^2 - a_n + 1$ and that, for arbitrary $k \in \mathbb{N}$,

$$\sum_{j=1}^{k} \frac{1}{a_j} \leq 1.$$

Therefore $\{a_j\}$ satisfies the conditions of Step 2.

Step 3. The sequence of integers $\{a_n\}$ defined in Exercise 11.10.5 is increasing since

$$a_{n+1} - a_n = a_n^2 - 2a_n + 1 = (a_n - 1)^2 > 0.$$

Define $k = k(n)$ to be the least integer such that $a_{k+1} > n$. Thus

$$2 = a_1 < a_2 < \cdots < a_k \leq n < a_{k+1} < \cdots . \tag{11.10.10}$$

Introduce the notation

$$b_j = \frac{n}{a_j} \tag{11.10.11}$$

and define

$$L_{n,k} = \frac{n!}{\lfloor b_1 \rfloor! \, \lfloor b_2 \rfloor! \cdots \lfloor b_k \rfloor!} \tag{11.10.12}$$

for $n \in \mathbb{N}$ and $k = k(n)$ as above. Observe that $\lfloor b_j \rfloor = 0$ if $j > k(n)$. Thus

$$L_{n,k} = \frac{n!}{\lfloor b_1 \rfloor! \, \lfloor b_2 \rfloor! \lfloor b_3 \rfloor! \cdots}. \tag{11.10.13}$$

Exercise 11.10.6. Prove that, for any n, $k \in \mathbb{N}$, the number $L_{n,k}$ is an integer. **Hint:** Use the multinomial expansion given in Exercise 2.11.2.

Lemma 11.10.7. *Let p be a prime. Then the p-adic valuation of $L_{n,k}$ satisfies*

$$\nu_p(L_{n,k}) \geq \lfloor \log_p n \rfloor . \tag{11.10.14}$$

It follows that $d_n \leq L_{n,k}$.

Proof. Legendre's series (2.6.1) gives

$$\nu_p(L_{n,k}) = \sum_{j=1}^{\lfloor \log_p n \rfloor} \left(\left\lfloor \frac{n}{p^j} \right\rfloor - \left\lfloor \frac{n}{a_1 p^j} \right\rfloor - \left\lfloor \frac{n}{a_2 p^j} \right\rfloor - \cdots - \left\lfloor \frac{n}{a_k p^j} \right\rfloor \right).$$

Take $x = n/p^j$ and $x_i = a_i$ in Step 1 to conclude that every term in the previous sum is at least 1. This gives the result. □

Note 11.10.8. The rest of the steps prove that $L_{n,k} \leq 3^n$.

Step 4. Continue with the notation $b_i = n/a_i$. Then

$$\frac{b_i^{b_i}}{\lfloor b_i \rfloor^{\lfloor b_i \rfloor}} < (eb_i)^{1-1/a_i}$$

holds for $n \geq a_i$.

Proof. For $n = a_i$ the inequality is clear. For $n > a_i$,

$$\begin{aligned} \frac{b_i^{b_i}}{\lfloor b_i \rfloor^{\lfloor b_i \rfloor}} &\leq \frac{b_i^{b_i}}{(b_i - 1 + 1/a_i)^{b_i - 1 + 1/a_i}} \\ &= \left(1 + \frac{a_i - 1}{n - a_i + 1}\right)^{\frac{n-a_i+1}{a_i-1} \cdot \frac{a_i-1}{a_i}} \times b_i^{1-1/a_i} \\ &< (eb_i)^{1-1/a_i}. \end{aligned}$$

Step 5. Define $c_i = \lfloor b_i \rfloor$. Then

$$L_{n,k} = \frac{n!}{c_1!\, c_2! \cdots c_k!}.$$

Then the inequality

$$L_{n,k} < \frac{n^n}{c_1^{c_1} \cdots c_k^{c_k}}$$

holds.

Proof. Let $m = m_1 + \cdots + m_r$. The multinomial theorem shows that

$$m^m = (m_1 + \cdots + m_r)^m > \frac{m!}{m_1!\, m_2! \cdots m_r!} m_1^{m_1} \cdots m_k^{m_k}. \tag{11.10.15}$$

Now recall that $k = k(n)$ is the least integer such that $a_{k+1} > n$ and $b_i = n/a_i$. Define

$$t = \sum_{i=1}^{k} \lfloor b_i \rfloor . \tag{11.10.16}$$

Then $k < t \leq n$. Indeed,

$$t \leq \sum_{i=1}^{k} \frac{n}{a_i} \leq n \sum_{i=1}^{k} \frac{1}{a_i} \leq n. \tag{11.10.17}$$

On the other hand, the sum defining t has k positive integers. Thus $t > k$. This implies that

$$L_{n,k} = \frac{n(n-1)\cdots(t+1)t!}{c_1!\cdots c_k!} < \frac{n^{n-t}t^t}{c_1!\cdots c_k!}$$

holds because $t! < t^t$.

Exercise 11.10.9. Use (11.10.15) to finish the proof of this step.

Step 6. Continue with the notation $a_k \leq n < a_{k+1}$. Then, for $k \geq 3$, the inequality $k < \log_2 \log_2 n + 2$ holds.

Proof. The recurrence $a_{k+1} = a_k^2 - a_k + 1$ implies $a_{k+1} > 2^{2^{k-1}} + 1$. This is the result.

Step 7. Let $k = k(n)$ and let t be defined as before. Then the inequality

$$L_{n,k} < \frac{n^n (eb_1)^{1-1/a_1} \cdots (eb_k)^{1-1/a_k}}{b_1^{b_1}\, b_2^{b_2} \cdots b_k^{b_k}}$$

holds.

Proof. Step 5 has given the inequality

$$L_{n,k} < \frac{n^n}{c_1^{c_1} \cdots c_k^{c_k}} \tag{11.10.18}$$

and Step 4 states that

$$\frac{1}{c_i^{c_i}} < \frac{1}{b_i^{b_i}} \left(eb_i\right)^{1-1/a_i}. \tag{11.10.19}$$

This gives the stated inequality.

Note 11.10.10. The last part of the proof consists of the study of the limit

$$w = \lim_{k \to \infty} a_1^{1/a_1}\, a_2^{1/a_2} \cdots a_k^{1/a_k}$$

and establishing the bound

$$L_{n,k} < e^{k-3/2} n^{k-3/2} w^n.$$

This will prove the bound $L_{n,k} < 3^n$. Lemma 11.10.7 will imply $d_n < 3^n$.

Step 8. Observe that the function $a_1^{1/a_1}a_2^{1/a_2}\cdots a_k^{1/a_k}$ is monotonically increasing as a function of k. Moreover, the recurrence $a_{i+1} = a_i^2 - a_i + 1$ gives $a_i^2 > a_{i+1} > (a_i - 1)^2$. Therefore

$$\frac{\log a_{i+1}^{1/a_{i+1}}}{\log a_i^{1/a_i}} = \frac{a_i \log a_{i+1}}{a_{i+1}\log a_i} < \frac{2a_i}{a_{i+1}} < \frac{2a_i}{(a_i-1)^2} < \frac{1}{2},$$

for all $i \geq 3$. The value $\log a_6^{1/a_6} < 5 \times 10^{-6}$ gives the bound

$$\sum_{i=1}^{\infty} \log a_i^{1/a_i} = \sum_{i=1}^{5} \log a_i^{1/a_i} + \sum_{i=6}^{\infty} \log a_i^{1/a_i} < 1.08240 + 10^{-5}.$$

Step 9. Define $w = \lim_{k\to\infty} a_1^{1/a_1}\, a_2^{1/a_2}\cdots a_k^{1/a_k}$. Then $w < 2.952$.

Exercise 11.10.11. Check the numerology.

Step 10. Observe the identities

$$\begin{aligned}\frac{a_1-1}{a_1} + \frac{a_2-1}{a_2} + \cdots + \frac{a_k-1}{a_k} &= 1 - 1/a_1 + \cdots + 1 - 1/a_k \\ &= k - \sum_{i=1}^{k} \frac{1}{a_i} \\ &= k - 1 + \frac{1}{a_{k+1}-1}.\end{aligned}$$

This implies

$$\begin{aligned}L_{n,k} &< \frac{(ne)^{k-1+1/(a_{k+1}+1)}\, w^n}{a_1^{1-1/a_1}a_2^{1-1/a_2}\cdots a_k^{1-1/a_k}} \\ &< e^{k-3/2}n^{k-3/2}w^n\end{aligned}$$

since $n \leq a_1a_2\cdots a_k$.

Exercise 11.10.12. Check the details.

Exercise 11.10.13. Prove that the inequality $L_{n,k} < e^{k-3/2}n^{k-3/2}w^n$ implies $L_{n,k} < 3^n$.

Lemma 11.10.7 completes the proof of the estimate $d_n < 3^n$. This establishes Theorem 11.10.1 and shows that $\ln 2$ is irrational.

Note 11.10.14. The bound $d_n < 3^n$ admits a simpler proof, provided one is willing to admit as known the **Prime Number Theorem**. This is one of the biggest achievements of the nineteenth century. It was conjectured by Legendre and Gauss at the end of the eighteenth century and proven, independently, by J. Hadamard and C. de la Vallée Poussin in 1896. The reader will find a nice historical perspective on this theorem in the survey paper by P. Bateman and H. Diamond [**41**] and a description of a clever shortcut by D. Newman [**234**] in the paper by D. Zagier [**318**].

Theorem 11.10.15. *Let $\pi(n)$ be the number of primes up to n. Then*

$$\lim_{n\to\infty} \frac{\pi(n)}{n/\ln n} = 1.$$

Observe that

$$d_n = \prod_{p \le n} p^{\alpha_p(n)} \tag{11.10.20}$$

where the product runs over all primes $p \le n$ and $\alpha_p(n)$ is the greatest integer i such that $p^i \le n$. An upper bound for d_n is obtained by replacing $p^{\alpha_p(n)}$ by n and since there are $\pi(n)$ terms in the product, it follows that

$$d_n \le n^{\pi(n)}. \tag{11.10.21}$$

The prime number theorem shows that $n^{\pi(n)} \le e^{(1+\epsilon)n}$ for any $\epsilon > 0$. Taking $\epsilon = \ln 3 - 1 \ge \frac{1}{11}$ gives the result.

11.11. Harmonic numbers

The current section presents the first class of rational numbers considered in this text: these are the **harmonic numbers**. A second class, the **Bernoulli numbers**, is presented in Chapter 13.

Definition 11.11.1. The **harmonic numbers** are defined by

$$H_n = 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}. \tag{11.11.1}$$

The notation

$$H_n = \frac{N_n}{D_n} \tag{11.11.2}$$

with $\gcd(N_n, D_n) = 1$ is employed. This is the reduced form of the rational number H_n.

The generating function. The first tool for the study of harmonic numbers is their generating function. This is obtained in an elementary manner.

Lemma 11.11.2. *Let $\{a_n\}$ be a sequence with generating function*

$$A(x) = \sum_{n=0}^{\infty} a_n x^n.$$

Then the generating function of the partial sums $b_n = a_0 + a_1 + \cdots + a_n$ is

$$B(x) = \frac{A(x)}{1-x}.$$

Proof. The expansion of the geometric series, stated in (11.1.2), gives

$$B(x) = \sum_{n=0}^{\infty} a_n x^n \times \sum_{k=0}^{\infty} x^k = \sum_{k,n} a_n x^{n+k}$$

and introducing the new index $r = n + k$, it follows that

$$B(x) = \sum_{r=0}^{\infty} \left(\sum_{k=0}^{r} a_k \right) x^r,$$

as claimed. □

Theorem 11.11.3. *The generating function of the harmonic numbers is*

$$\sum_{n=0}^{\infty} H_n x^n = -\frac{\ln(1-x)}{1-x}. \tag{11.11.3}$$

Proof. The harmonic numbers are the partial sums of the sequence $\{1/n\}$. The result follows from Lemma 11.11.2 and the expansion $\displaystyle\sum_{n=1}^{\infty} \frac{x^n}{n} = -\ln(1-x)$, obtained by integrating $\displaystyle\sum_{n=0}^{\infty} x^n = \frac{1}{1-x}$. □

Exercise 11.11.4. Prove the identity

$$\sum_{n=0}^{\infty} \frac{H_n}{2^n} = 2\ln 2.$$

Exercise 11.11.5. Show that there is no sequence of numbers $\{a_k\}_{k=1}^{N}$, with fixed N, such that the recurrence

$$\sum_{k=1}^{N} a_k \frac{H_{n-k}}{(n-k)!} = 0$$

is valid for all $n \in \mathbb{N}$.

Arithmetical properties of harmonic numbers. The discussion of arithmetical properties of the harmonic numbers starts by showing that $H_n \notin \mathbb{N}$.

Theorem 11.11.6. *The harmonic numbers H_n, for $n > 1$, are not integers.*

Proof. Assume $H_n \in \mathbb{N}$ and let 2^k be the highest power of 2 less than or equal to n. Then

$$2^{k-1}H_n - \frac{1}{2} = 2^{k-1}\left(1 + \frac{1}{2} + \cdots + \frac{1}{2^k-1}\right) + 2^{k-1}\left(\frac{1}{2^k+1} + \cdots + \frac{1}{n}\right)$$

is a fraction with odd denominator. This is a contradiction: any fraction of the form $m - \frac{1}{2}$, with $m \in \mathbb{N}$, has even denominator. □

The denominator of H_n is a divisor of the least common multiple of $\{1, 2, \ldots, n\}$. This has been denoted by d_n in Theorem 11.10.1. The graph in Figure 11.11.1 shows the function

$$f(n) := \frac{1}{n} \left|\{1 \leq k \leq n : \text{denominator of } H_k = d_k\}\right|.$$

The function $f(n)$ measures the proportion of values where there is no cancellation in adding the terms forming H_n.

Wolstenholme's theorem. This result is one of the classic theorems on divisibility properties of the harmonic number H_n. Recall the notation $H_n = N_n/D_n$, with $\gcd(N_n, D_n) = 1$.

The first result, due to J. Wolstenholme [**314**], has already appeared in Theorem 2.5.18 in the discussion of the binomial coefficient

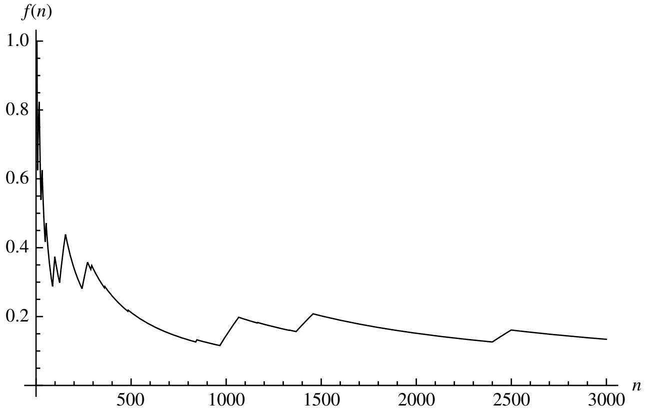


Figure 11.11.1. Proportion of harmonic numbers with denominator $\text{lcm}\{1, 2, \ldots, n\}$.

$\binom{2p-1}{p-1}$. The theorem states that, for $p > 3$ prime, the rational number H_{p-1} has a numerator divisible by p^2. The first result deals with divisibility by p.

Theorem 11.11.7. *Let $p > 3$ be a prime. Then p divides N_{p-1}.*

Proof. An alternative form of the result is that

$$1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p-1} \equiv 0 \mod p. \tag{11.11.4}$$

To check this, let $x_i \in \{1, 2, \ldots, p-1\}$ be the inverse of i modulo p, that is, $ix_i \equiv 1 \bmod p$. Then

$$N_{p-1} \equiv x_1 + x_2 + \cdots + x_{p-1} \mod p. \tag{11.11.5}$$

The numbers 1 and $p-1$ are the only ones for which $i = x_i$. Therefore as sets

$$\{1, 2, \ldots, p-2, p-1\} = \{x_1 = 1, x_2, \ldots, x_{p-2}, x_{p-1} = p-1\}.$$

It follows that

$$x_1 + x_2 + \cdots + x_{p-1} = 1 + 2 + \cdots + (p-1) = \frac{p(p-1)}{2},$$

and this is divisible by p. □

Exercise 11.11.8. Let p be a prime number. Define the numbers s_i by the expansion

$$(x-1)(x-2)\cdots(x-p+1) = x^{p-1} - s_1x^{p-2} + s_2x^{p-3} + \cdots + s_{p-1}.$$

Prove that $s_i \equiv 0 \bmod p$ for $1 \leq i \leq p-3$.

The next result improves Theorem 11.11.7 and deals with divisibility by p^2.

Theorem 11.11.9. *Let $p > 3$ be a prime. Then p^2 divides N_{p-1}.*

Proof. Replace $x = p$ in the factorization given in Exercise 11.11.8 and $s_{p-1} = (p-1)!$ to obtain

$$p^{p-2} - s_1p^{p-3} + \cdots + s_{p-3}p - s_{p-2} = 0. \tag{11.11.6}$$

Therefore p^2 divides s_{p-2}. The result follows from the identity

$$s_{p-2} = (p-1)!\, H_{p-1}. \tag{11.11.7}$$

□

Exercise 11.11.10. Check the details.

Modular properties of the numerator of H_n. The results of the previous section show that, for p prime, the number N_{p-1}, the numerator of H_{p-1}, is divisible by p. An interesting phenomenon has appeared in the study of the distribution of N_j taken modulo a given integer q.

Consider the sets

$$\mathrm{A}_q = \{N_j \bmod q : j \in \mathbb{N}\} \setminus \{0\},$$

the list of nonzero remainders of numerators of harmonic numbers modulo q, and

$$\mathrm{B}_q = \{j : 1 \leq j \leq q \text{ such that } \gcd(j,q) = 1\},$$

the set of numbers relatively prime to the modulus q.

Example 11.11.11. For $q = 11$, the two sets agree:

$$A_{11} = B_{11} = \{1,\, 2,\, 3,\, 4,\, 5,\, 6,\, 7,\, 8,\, 9,\, 10\}.$$

On the other hand, for $q = 15$,

$$A_{15} = \{1,\, 2,\, 3,\, 4,\, 5,\, 7,\, 8,\, 10,\, 11,\, 12,\, 13,\, 14\}$$

and

$$B_{15} = \{1, 2, 4, 7, 8, 11, 13, 14\}.$$

The graph in Figure 11.11.2 shows the sets A_{83} and A_{84}. This suggested looking at the values appearing in the A_q.

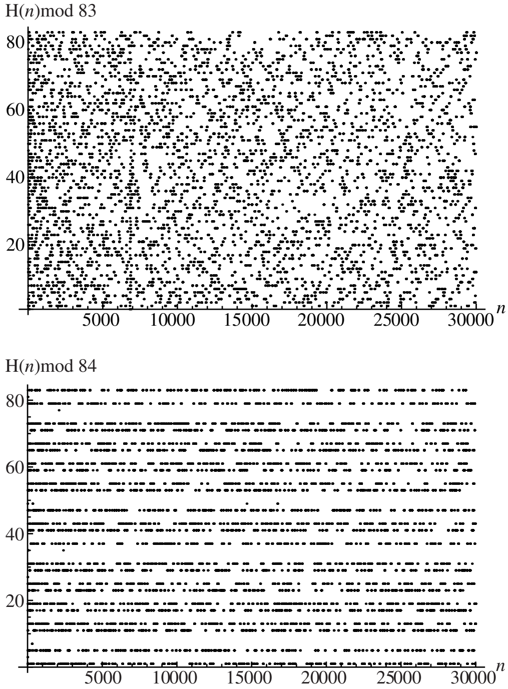


Figure 11.11.2. The distribution of numerators modulo 83 and 84.

Observe the granular structure for $q = 83$ and the band structure for $q = 84$. The reader should be careful with computer experiments for this problem. For example, for $q = 83$, the remainder 8 appears for the first time at position 1277. Therefore, the set A_q should be computed for sufficiently large size. The experiments seem to indicate that the following statements are true.

Conjecture 11.11.12. *The inclusion $B_q \subset A_q$ holds. Moreover, equality holds if and only if q is either a prime or a power of* 2.

Chapter 12

Trigonometric Functions

12.1. Introduction

The class of elementary functions include, up to now, polynomials, rational functions, exponentials, and logarithms. This class is now enlarged by a class of functions that the reader must have found in introductory courses and those that appear in the study of trigonometry. This chapter begins with a discussion of **sine** and **cosine** as the two most basic functions in this class. The definition requires the notion of **angle** and a preliminary discussion of it is given in terms of the length of the corresponding arc. The definition of angle, given in terms of the integral for arclength, gives an easy point of entry to the well-known properties of trigonometric functions.

12.2. The notion of angle

The basic variable of trigonometric functions is an **angle**. This is now introduced as the length of a chord on the unit circle.

Let $m \in \mathbb{R}^+$ and consider the point of intersection of the part of the line $y = mx$ in the first quadrant and the unit circle $x^2 + y^2 = 1$.

A simple calculation shows

$$x(m) = \frac{1}{\sqrt{1+m^2}} \quad \text{and} \quad y(m) = \frac{m}{\sqrt{1+m^2}}. \tag{12.2.1}$$

The angle associated to the slope m is defined next.

Definition 12.2.1. Let $m \in \mathbb{R}^+$. The **angle associated to** m is the value

$$\alpha(m) = \int_{(1+m^2)^{-1/2}}^{1} \frac{dt}{\sqrt{1-t^2}}. \tag{12.2.2}$$

This definition has the value $\alpha(0) = 0$ included in (12.2.2). The function α is extended to $m \in \mathbb{R}$ as an odd function. That is, for $m < 0$,

$$\alpha(-m) := -\alpha(m). \tag{12.2.3}$$

Exercise 12.2.2. Prove that α is a differentiable function and that

$$\alpha'(m) = \frac{1}{1+m^2}. \tag{12.2.4}$$

Establish first the continuity of α.

The function α is strictly increasing from $\alpha(0) = 0$ to its limiting value

$$\alpha(\infty) = \int_0^1 \frac{dt}{\sqrt{1-t^2}}, \tag{12.2.5}$$

corresponding to the length of a quarter of circle. This motivates the next definition.

Definition 12.2.3. The number π is defined by

$$\pi = 2\int_0^1 \frac{dt}{\sqrt{1-t^2}}.$$

Exercise 12.2.4. Use some simple geometric figures to bound the circle and conclude that

$$2\sqrt{2} < \pi < 4. \tag{12.2.6}$$

Exercise 12.2.5. Let $A(r)$ and $L(r)$ denote the area and length of a circle of radius r, respectively. Scale the integrals to check that $A(r) = A(1)r^2$ and $L(r) = L(1)r$. Now integrate by parts to show that $L(1) = 2A(1)$. This confirms that the π appearing in the formula for the area of a circle is the same constant in the expression for its length.

12.3. Sine and cosine

The two basic trigonometric functions are introduced next.

Definition 12.3.1. Let $x \in [0, \pi/2]$. The **sine** of the angle x is defined by

$$\sin x = \frac{m}{\sqrt{1+m^2}} \tag{12.3.1}$$

where $m \in \mathbb{R}^+$ is the unique positive real number such that $\alpha(m) = x$. The function **cosine** of the **angle** x is defined by

$$\cos x = \frac{1}{\sqrt{1+m^2}}. \tag{12.3.2}$$

Note 12.3.2. Observe that $m = \alpha^{-1}(x)$ and Exercise 12.2.2 shows that α is a differentiable function. Differentiabilty properties of the trigonometric functions now follow from the inverse function theorem, Theorem 11.8.1.

The definition of these functions show that the point of coordinates $(u, v) = (\cos x, \sin x)$ is on the circle $u^2 + v^2 = 1$.

Special values of functions play an important role in their study. The next exercise establishes some well-known examples.

Exercise 12.3.3. The special value $\sin 0 = 0$ comes directly from $\alpha(0) = 0$, and $\alpha(\infty) = \frac{\pi}{2}$ shows that $\sin \frac{\pi}{2} = 1$. Then $\cos 0 = 1$ and $\cos \frac{\pi}{2} = 0$. Prove that $\alpha(1) = \pi/4$ yields $\sin \frac{\pi}{4} = 1/\sqrt{2}$. Conclude that $\cos \frac{\pi}{4} = 1/\sqrt{2}$. **Hint:** You need to check the identity

$$\int_{1/\sqrt{2}}^{1} \frac{dt}{\sqrt{1-t^2}} = \frac{1}{2} \int_0^1 \frac{dt}{\sqrt{1-t^2}}. \tag{12.3.3}$$

The change of variables $s = t^2$ shows that the second integral is symmetric with respect to $s = 1/2$.

Note 12.3.4. An interesting question related to special values is, *for which rational multiples of π do the trigonometric functions take rational values*? Everyone knows vaues like $\sin\frac{\pi}{6} = \frac{1}{2}$ and $\tan\frac{\pi}{4} = 1$, and it turns out that these (along with the values producing 0) are essentially the only choices. The reader will find a proof of this result in [**227**].

Exercise 12.3.5. Prove that

$$\frac{d}{dx}\sin x = \cos x \tag{12.3.4}$$

and from $\sin^2 x + \cos^2 x = 1$ deduce that

$$\frac{d}{dx}\cos x = -\sin x. \tag{12.3.5}$$

Hint: Differentiate the relation $\sin\alpha(m) = m/\sqrt{1+m^2}$.

Exercise 12.3.6. Compute a closed form for the derivatives of the functions sine and cosine. Taylor's theorem, Theorem 2.4.1, now yields the power series expansions

$$\sin x = \sum_{k=0}^{\infty}(-1)^k\frac{x^{2k+1}}{(2k+1)!}$$

and

$$\cos x = \sum_{k=0}^{\infty}(-1)^k\frac{x^{2k}}{(2k)!}.$$

Characterization of trigonometric functions by differential equations. The exponential function $f(x) = e^x$ is the only function satisfying

$$\begin{aligned} f'(x) &= f(x), \\ f(0) &= 1. \end{aligned} \tag{12.3.6}$$

This appeared as Theorem 11.2.3. This section presents a similar characterization for trigonometric functions.

Theorem 12.3.7. *The function $f(x) = a\cos x + b\sin x$ is the unique solution to*

$$\begin{aligned} f''(x) &= -f(x), \\ f(0) &= a, \\ f'(0) &= b. \end{aligned}$$

Proof. For a, $b \in \mathbb{R}$ define

$$E(x) = (f(x) - a\cos x - b\sin x)^2 + (f'(x) + a\sin x - b\cos x)^2 .$$

A direct calculation shows that

$$E'(x) = 2(f'(x) + a\sin x - b\cos x)\,(f''(x) + f(x)) = 0.$$

It follows that E is constant and the form of $f(x)$ has been established. □

The relation to exponentials: A formula of Euler. The power series of the exponential

$$e^x = \sum_{k=0}^{\infty} \frac{x^k}{k!} \tag{12.3.7}$$

is now employed to provide a remarkable relation between the exponential function and the trigonometric functions.

Theorem 12.3.8. *Let $x \in \mathbb{R}$ and let i be the imaginary unit. Then*

$$e^{ix} = \cos x + i\sin x. \tag{12.3.8}$$

Proof. The expansion (12.3.7) gives

$$e^{ix} = \sum_{k=0}^{\infty} i^k \frac{x^k}{k!}. \tag{12.3.9}$$

The result now follows from the expressions

$$i^{4k} = 1, \quad i^{4k+1} = i, \quad i^{4k+2} = -1, \quad i^{4k+3} = -i$$

for the integer powers of i and the power series given in Exercise 12.3.6. □

Exercise 12.3.9. Check that $e^{i\pi} + 1 = 0$. This is a relation among five fundamental constants: 0, 1, i, e, and π.

The next exercise will be useful in the solution of cubic polynomial equations presented in Section 12.10.

Exercise 12.3.10. Let $c \in \mathbb{C}$. Prove that the equation $\sin x = c$ always has a solution. **Hint:** Write $\sin x = (e^{ix} - e^{-ix})/(2i)$.

12.4. The additional trigonometric functions

In this section the remaining classical trigonometric functions are described.

Definition 12.4.1. The **tangent** of the angle α is defined by

$$\tan\alpha = \frac{\sin\alpha}{\cos\alpha}. \tag{12.4.1}$$

In addition, the **cotangent** of α is defined by

$$\cot\alpha = \frac{\cos\alpha}{\sin\alpha}. \tag{12.4.2}$$

Note that $\cot\alpha = 1/\tan\alpha$. The functions **secant** and **cosecant**, defined by

$$\sec\alpha = \frac{1}{\cos\alpha} \quad \text{and} \quad \csc\alpha = \frac{1}{\sin\alpha}, \tag{12.4.3}$$

complete the traditional list of six trigonometric functions.

Note 12.4.2. Observe that (12.3.1) and (12.3.2) give

$$\tan\alpha(m) = m. \tag{12.4.4}$$

Conclude that $\alpha(m)$ is the inverse of $\tan\alpha$. This function will be denoted by arctan x. Exercise 12.2.2 gives

$$\frac{d}{dx}\text{arctan } x = \frac{1}{1+x^2}. \tag{12.4.5}$$

Exercise 12.4.3. Verify the identity

$$\text{arctan } x = \sum_{k=0}^{\infty}(-1)^k \frac{x^{2k+1}}{2k+1}.$$

Use $x = 1$ to obtain the **Leibnitz series** for π:

$$\frac{\pi}{4} = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \cdots .$$

Estimate the error after n terms in the series.

12.4.1. The tangent numbers.

The discussion of the tangent function begins with its power series expansion.

Theorem 12.4.4. *The **tangent numbers** T_n, defined by the expansion*

$$\tan x = \sum_{n=0}^{\infty} T_n \frac{x^n}{n!}, \tag{12.4.6}$$

satisfy $T_{2n} = 0$ and $T_{2n+1} > 0$.

Proof. The value $T_0 = 0$ comes from evaluating

$$\tan(\arctan x) := \sum_{n=0}^{\infty} \frac{T_n}{n!} (\arctan x)^n = x, \tag{12.4.7}$$

at $x = 0$. Differentiate with respect to x to obtain

$$\sum_{n=0}^{\infty} \frac{T_{n+1}}{n!} (\arctan x)^n = 1 + x^2, \tag{12.4.8}$$

and replace $x = 0$ to conclude that $T_1 = 1$. Differentiating again yields

$$\sum_{n=0}^{\infty} \frac{T_{n+2}}{n!} (\arctan x)^n = 2x(1 + x^2), \tag{12.4.9}$$

which gives $T_2 = 0$. The general case uses the operator

$$D = (1 + x^2) \frac{d}{dx}. \tag{12.4.10}$$

Then (12.4.9) can be written as

$$\sum_{n=0}^{\infty} \frac{T_{n+2}}{n!} (\arctan x)^n = D(1 + x^2). \tag{12.4.11}$$

Exercise 12.4.5. Define the family of polynomials

$$A_k(x) = D^{(k)}(1 + x^2). \tag{12.4.12}$$

Prove they satisfy the recurrence

$$A_{k+1}(x) = 2x(1 + x^2) \frac{d}{dx} A_{k-1}(x) + (1 + x^2)^2 \frac{d^2}{dx^2} A_{k-1}(x). \tag{12.4.13}$$

Repeated differentiation yields

$$\sum_{n=0}^{\infty} \frac{T_{n+k}}{n!}(\arctan x)^n = D^{(k-1)}(1+x^2) = A_{k-1}(x), \tag{12.4.14}$$

and this gives $T_{n+1} = A_n(0)$. The facts that $T_{2n} = 0$ and $T_{2n+1} > 0$ follow by evaluating at $x = 0$ and using the recurrence (12.4.5) with the initial values $T_0 = 0$ and $T_1 = 1$. □

Exercise 12.4.6. Prove that the coefficients T_n are rational numbers. Chapter 13 will express them in terms of Bernoulli numbers B_{2n}. Exercise 13.3.23 gives the identity

$$T_n = \begin{cases} 0 & \text{if } n \text{ is even,} \\ (-1)^{(n-1)/2} 2^{n+1}(2^{n+1}-1)\,\frac{B_{n+1}}{n+1} & \text{if } n \text{ is odd.} \end{cases}$$

12.4.2. A sequence of polynomials. The identity

$$\frac{d}{dx}\tan x = \sec^2 x = 1 + \tan^2 x \tag{12.4.15}$$

shows that there exists a polynomial P_n such that

$$\left(\frac{d}{dx}\right)^n \tan x = P_n(\tan x). \tag{12.4.16}$$

A second family of polynomials, $Q_n(x)$, appears from

$$\left(\frac{d}{dx}\right)^n \sec x = Q_n(\tan x)\,\sec x. \tag{12.4.17}$$

The names **tangent polynomials** and **secant polynomials** are employed for $P_n(x)$ and $Q_n(x)$, respectively. This section follows the papers by M. E. Hoffman [**172, 173**] to describe some properties of these polynomials.

The discussion begins with an elementary lemma. The proof is left to the reader.

Lemma 12.4.7. *Assume f is a function such that $f'(x) = P(f(x))$ for a polynomial P. Then there is a family of polynomials $\{P_n(x)\}$ such that $f^{(n)}(x) = P_n(f(x))$. The polynomials P_n satisfy the recurrence $P_{n+1}(u) = P_n'(u)P(u)$ and $P_0(u) = u$.*

Introduce the exponential generating function

$$F(u,t) = \sum_{n=0}^{\infty} P_n(u)\,\frac{t^n}{n!}. \tag{12.4.18}$$

Lemma 12.4.7 produces a differential equation for F.

Lemma 12.4.8. *The function $F(u,t)$ is characterized by*

$$\frac{\partial F}{\partial t} = P(u)\frac{\partial F}{\partial u}$$

with initial condition $F(u,0) = u$.

The special case of $P(u) = u^2 + 1$ produces the tangent polynomials. As in this case, in the general situation, there is an analog of the function $\sec x$.

Lemma 12.4.9. *Assume $f(x)$ as in Lemma 12.4.7. Define*

$$g(x) = \exp \int f(x)\,dx.$$

Then $g'(x) = f(x)g(x)$ and there is a family of polynomials $\{Q_n(x)\}$ such that $g^{(n)}(x) = Q_n(f(x))g(x)$. These polynomials satisfy the recurrence

$$Q_{n+1}(u) = uQ_n(u) + P(u)Q_n'(u).$$

The corresponding generating function

$$G(u,t) = \sum_{n=0}^{\infty} Q_n(u)\,\frac{t^n}{n!} \tag{12.4.19}$$

is characterized by

$$\frac{\partial G}{\partial t} = P(u)\frac{\partial G}{\partial u} + uG(u)$$

with initial condition $G(u,0) = 1$.

The next result gives an explicit formula for F and G.

Theorem 12.4.10. *The exponential generating functions in* (12.4.18) *and* (12.4.19) *are given by*

$$F(u,t) = f(f^{-1}(u) + t)$$

and

$$G(u,t) = \frac{g(f^{-1}(u)+t)}{g(f^{-1}(u))}.$$

Proof. Replace the stated forms in the partial differential equations that characterize F and G. □

Example 12.4.11. In the case $f(x) = \tan x$, the companion function is $g(x) = \sec x$. Theorem 12.4.10 gives

$$F(u,t) = \frac{\sin t + u \cos t}{\cos t - u \sin t} \quad \text{and} \quad G(u,t) = \frac{1}{\cos t - u \sin t}.$$

Exercise 12.4.12. Prove that the functions $F(u,t)$ and $G(u,t)$ are characterized by the system of equations

$$\frac{\partial F}{\partial t} = P(F) \quad \text{and} \quad \frac{\partial G}{\partial t} = FG,$$

with the initial conditions $F(u,0) = u$ and $G(u,0) = 1$.

Exercise 12.4.13. Prove that if $P(u) = u^2+1$, then the polynomials P_n, Q_n from Lemmas 12.4.7 and 12.4.8 satisfy the recurrences:

$$\begin{aligned} P_{n+1}(u) &= \sum_{i=0}^{n} \binom{n}{i} P_i(u) P_{n-i}(u) + \delta_{0,n}, \\ Q_{n+1}(u) &= \sum_{i=0}^{n} P_i(u) Q_{n-i}(u), \end{aligned}$$

where $\delta_{0,n}$ is Kronecker's delta (1 if $n = 0$ and 0 otherwise).

The final result from the paper [**172**] stated here is a relation that allows the computation of $P_n(u)$, $Q_n(u)$ at $u = 1$ in terms of the values at $u = 0$.

Theorem 12.4.14. *Assume* $P(u) = u^2 + 1$. *Then*

$$P_n(u) = 2^n \left[P_n\left(\frac{u^2-1}{2u}\right) + \frac{u^2+1}{2u}\, Q_n\left(\frac{u^2-1}{2u}\right) \right]$$

and

$$P_{n+1}(u) = (u^2+1) \sum_{i=0}^{n} \binom{n}{i} Q_i(u) Q_{n-i}(u).$$

Corollary 12.4.15. *The values at* $u = 0$ *and* $u = 1$ *of the polynomials* P_n *and* Q_n *in Theorem* 12.4.14 *satisfy the relations*

$$P_n(1) = \begin{cases} 2^n Q_n(0) & \textit{if } n \textit{ is even}, \\ 2^n P_n(0) & \textit{if } n \textit{ is odd} \end{cases}$$

and

$$Q_n(1) = \frac{1}{2}P_{n+1}(1) - \sum_{i=0}^{n-1} \binom{n}{i} Q_i(1)Q_{n-i}(1).$$

Exercise 12.4.16. Prove that the tangent numbers T_n, defined in (12.4.6), satisfy the recurrence

$$T_{n+1} = \sum_{i=0}^{n} \binom{n}{i} T_i T_{n-i}$$

with initial condition $T_1 = 1$. In particular, T_n is a positive integer.

Note 12.4.17. The tangent numbers T_n are expressed in terms of the Bernoulli numbers in Exercise 13.3.23.

Exercise 12.4.18. Examine the arithmetical properties of the tangent numbers. For instance, prove that

$$\nu_2(T_{2n+1}) = 2n - \nu_2(n+1).$$

12.4.3. A combinatorial interpretation. The tangent numbers T_n admit an interpretation in terms of **alternating permutations**. This concept is introduced next.

Definition 12.4.19. Let $w = w_1w_2\cdots w_n$ be a sequence of n distinct numbers. The sequence is called **alternating** if $w_1 > w_2 < w_3 > w_4 \cdots$ and **reverse alternating** if $w_1 < w_2 > w_3 < w_4 \cdots$.

From now on it is assumed that the numbers $\{w_1, \ldots, w_n\}$ form a permutation of $\{1, 2, \ldots, n\}$.

Exercise 12.4.20. Prove that the number of alternating permutations is the same as the number of reverse alternating permutations. **Hint:** If w is an alternating permutation, define $w_i^* = n + 1 - w_i$.

Let e_n be the number of alternating permutations. The goal is to relate e_n to the tangent numbers. Given $0 \leq k \leq n$, choose a subset $S \subset \{1, 2, \ldots, n\}$ with k elements. This can be done in $\binom{n}{k}$ ways. Let $S^* = \{1, 2, \ldots, n\} \setminus S$. Choose a reverse alternating permutation of S in e_k ways and an alternating permutation of S^* in e_{n-k} ways. Now form the word $w = u^r, n+1, v$, where u^r is the word u written backwards.

Exercise 12.4.21. Convince yourself that the words w constructed above contain every alternating and every reverse alternating permutation of $n+1$ symbols. Conclude that

$$2e_{n+1} = \sum_{k=0}^{n} e_k e_{n-k}. \tag{12.4.20}$$

Define the exponential generating function

$$y(x) = \sum_{k=0}^{\infty} \frac{e_k}{k!} x^k. \tag{12.4.21}$$

Exercise 12.4.22. Prove that the result of Exercise 12.4.21 yields the differential equation

$$2y'(x) = y^2 + 1 \tag{12.4.22}$$

with the initial condition $y(0) = 1$. Solve the equation to obtain

$$y(x) = \tan x + \sec x. \tag{12.4.23}$$

Conclude that T_{2n-1} is the number of alternating permutations in $2n-1$ symbols.

Note 12.4.23. For a permutation w of $\{1, 2, \ldots, n\}$ the set

$$D(w) = \{i : 1 \leq i \leq n-1 \text{ and } w_i > w_{i+1}\} \tag{12.4.24}$$

is called the **descent set** of w and $\text{des}(w) = |D(w)|$ is the **descent number** of w. The polynomial

$$A_n(w) = \sum_{w} x^{1+\text{des}(w)} := \sum_{k} A_{n,k} x^k \tag{12.4.25}$$

is the **Eulerian polynomial** defined in (4.2.22). The coefficients $A_{n,k}$ count the number of permutations of n numbers with exactly k descents. R. Stanley [**280**] calls this an example of **combinatorial trigonometry**.

12.5. The addition theorem

A function f is said to have an **addition theorem** if $f(x+y)$ can be expressed in terms of $f(x)$ and $f(y)$. The type of functions required to express $f(x+y)$ is used to label the addition theorem. For instance, the relation

$$e^{x+y} = e^x \cdot e^y \tag{12.5.1}$$

shows that the exponential function satisfies a *polynomial* addition theorem. The classical result for trigonometric functions is given next.

Theorem 12.5.1. *The trigonometric functions satisfy*

$$\begin{aligned} \sin(x+y) &= \sin x \cos y + \cos x \sin y \\ &= \sin x \sqrt{1-\sin^2 y} + \sqrt{1-\sin^2 x}\, \sin y. \end{aligned}$$

Similarly

$$\begin{aligned} \cos(x+y) &= \cos x \cos y - \sin x \sin y \\ &= \cos x\, \cos y - \sqrt{1-\cos^2 x}\, \sqrt{1-\cos^2 y}. \end{aligned}$$

Proof. Fix $y \in \mathbb{R}$. Then $f(x) = \sin(x+y)$ satisfies the differential equation $f''(x) + f(x) = 0$ and has initial conditions $f(0) = \sin y$ and $f'(0) = \cos y$. Theorem 12.3.7 gives the result. The formula for $\cos(x+y)$ is established in the same manner. □

Exercise 12.5.2. Prove the addition theorem by writing

$$\sin x = \frac{e^{ix} - e^{-ix}}{2i} \quad \text{and} \quad \cos x = \frac{e^{ix} + e^{-ix}}{2} \tag{12.5.2}$$

and using the addition theorem for the exponential function.

Exercise 12.5.3. Use the addition theorem to prove that $\sin x$ and $\cos x$ are periodic functions of period 2π.

Corollary 12.5.4. *There are polynomials R_m, S_m such that*

$$\cos mx = R_m(\cos x) \tag{12.5.3}$$

and

$$\sin mx = \begin{cases} S_m(\sin x) & \textit{if } m \textit{ is odd,} \\ S_m(\sin x) \cos x & \textit{if } m \textit{ is even.} \end{cases} \tag{12.5.4}$$

The polynomials satisfy the recurrences

$$R_{m+1}(t) = 2tR_m(t) - R_{m-1}(t) \tag{12.5.5}$$

and

$$(12.5.6) \quad S_{m+1}(t) = \begin{cases} -S_{m-1}(t) + 2(1-t^2)S_m & \textit{if } m \textit{ is odd,} \\ -S_{m-1}(t) + 2S_m & \textit{if } m \textit{ is even.} \end{cases}$$

The initial values are $R_0(t) = 1$, $S_0(t) = 0$, $R_1(t) = S_1(t) = t$.

Proof. The existence of the polynomials and the recurrences follow directly from the identities

$$\begin{aligned} \cos((m+1)x) + \cos((m-1)x) &= 2\cos x \cos mx, \\ \sin((m+1)x) + \sin((m-1)x) &= 2\cos x \sin mx. \end{aligned}$$

□

Exercise 12.5.5. Check that $R_m(1) = 1$. Evaluate $S_m(1)$.

The polynomials R_m and S_m have integer coefficients. The first few are

$$\begin{array}{lcl lcl} R_0(t) & = & 1, & S_0(t) & = & 0, \\ R_1(t) & = & t, & S_1(t) & = & t, \\ R_2(t) & = & 2t^2 - 1, & S_2(t) & = & 2t, \\ R_3(t) & = & 4t^3 - 3t, & S_3(t) & = & -4t^3 + 3t, \\ R_4(t) & = & 8t^4 - 8t + 1, & S_4(t) & = & -8t^3 + 4t, \\ R_5(t) & = & 16t^5 - 20t^3 + 5t, & S_5(t) & = & 16t^5 - 20t^3 + 5t, \\ R_6(t) & = & 32t^6 - 48t^4 + 18t^2 - 1, & S_6(t) & = & 32t^5 - 32t^3 + 6t. \end{array}$$

Note 12.5.6. The polynomials R_n, S_n are the **Chebyshev polynomials** that will be analyzed in Chapter 14.

Exercise 12.5.7. The addition theorem in now employed to produce a formula for π due to F. Vieta [**298**]. The argument starts with

$$\sin x = 2\cos\frac{x}{2}\sin\frac{x}{2}.$$

Iterate this relation to produce

$$\sin x = 2^n \sin\frac{x}{2^n} \times \prod_{k=1}^{n} \cos\frac{x}{2^k}.$$

Now use the relation $\cos \frac{x}{2} = \sqrt{\frac{1}{2} + \frac{1}{2}\cos x}$ to produce

$$\cos \frac{x}{2^k} = \sqrt{\frac{1}{2} + \frac{1}{2}\sqrt{\frac{1}{2} + \frac{1}{2}\sqrt{\frac{1}{2} + \cdots + \frac{1}{2}\sqrt{\frac{1}{2} + \frac{1}{2}\cos x}}}},$$

with k radicals in the formula. An expression for $\sin x/(2^n \sin x/2^n)$ as a finite product of radicals follows from here. Pass to the limit to obtain

$$\frac{\sin x}{x} = \prod_{k=1}^{\infty} \sqrt{\frac{1}{2} + \frac{1}{2}\sqrt{\frac{1}{2} + \frac{1}{2}\sqrt{\frac{1}{2} + \cdots + \frac{1}{2}\sqrt{\frac{1}{2} + \frac{1}{2}\cos x}}}},$$

where the kth term contains k nested radicals. The special choice of $x = \pi/2$ gives **Vieta's formula**

$$\frac{2}{\pi} = \sqrt{\frac{1}{2}}\sqrt{\frac{1}{2} + \frac{1}{2}\sqrt{\frac{1}{2}}}\sqrt{\frac{1}{2} + \frac{1}{2}\sqrt{\frac{1}{2} + \frac{1}{2}\sqrt{\frac{1}{2}}}} \cdots .$$

Check the error term after multiplying 100 terms in the product.

12.6. Stirling's formula and π

Chapter 9 was dedicated to the evaluation of Wallis' formula

$$W_n = \int_0^{\pi/2} \cos^{2n}\theta \, d\theta = 2^{-2n}\binom{2n}{n}\frac{\pi}{2}.$$

In this chapter the integral

$$I_n = \int_0^{\pi/2} \cos^n x \, dx \tag{12.6.1}$$

is evaluated in closed form.

Lemma 12.6.1. *The integral I_n satisfies the recurrence*

$$I_n = \frac{n-1}{n} I_{n-2}. \tag{12.6.2}$$

Proof. Integrate by parts to obtain

$$\begin{aligned} I_n &= \int_0^{\pi/2} \cos^{n-1} x \, \cos x \, dx \\ &= (n-1) \int_0^{\pi/2} \cos^{n-2} x \, \sin^2 x \, dx. \end{aligned}$$

Now use $\sin^2 x = 1 - \cos^2 x$ to obtain the result. □

Exercise 12.6.2. Iterate the recurrence (12.6.2) to obtain

$$I_{2n+1} = \frac{2^{2n}\,(n!)^2}{(2n+1)!} = \frac{2^{2n}}{(2n+1)\binom{2n}{n}}$$

and

$$I_{2n} = \frac{(2n)!}{2^{2n+1}\,(n!)^2}\pi = \frac{1}{2^{2n}}\binom{2n}{n}\frac{\pi}{2},$$

using the values $I_0 = \pi/2$ and $I_1 = 1$. The integral I_{2n} is the Wallis case W_n. Check directly that $I_{2n+1} < I_{2n} < I_{2n-1}$ and confirm the relation

$$\frac{I_{2n+1}}{I_{2n-1}} = \frac{2n}{2n+1} \to 1 \quad \text{as } n \to \infty.$$

Conclude that $I_{2n}/I_{2n+1} \to 1$. Now check that

$$\frac{I_{2n+1}}{I_{2n}} = \frac{2 \cdot 2 \cdot 4 \cdot 4 \cdot 6 \cdot 6 \cdots (2n) \cdot (2n)}{1 \cdot 3 \cdot 3 \cdot 5 \cdot 5 \cdot 7 \cdot 7 \cdots (2n-1) \cdot (2n-1)(2n+1)} \times \frac{2}{\pi}$$

and prove **Wallis' infinite product** for π:

$$\frac{\pi}{2} = \frac{2}{1}\,\frac{2}{3}\,\frac{4}{3}\,\frac{4}{5}\,\frac{6}{5}\,\frac{6}{7}\,\frac{8}{7}\,\frac{8}{9}\,\frac{10}{9}\,\frac{10}{11}\,\frac{12}{11}\,\frac{12}{13}\,\frac{14}{13}\,\frac{14}{15}\,\frac{16}{15}\,\frac{16}{17}\cdots. \tag{12.6.3}$$

More examples of infinite products related to constants of analysis appear in Chapter 16.

Exercise 12.6.3. Confirm that Wallis' product implies the asymptotics

$$c_n := \binom{2n}{n} \sim \frac{2^{2n}}{\sqrt{\pi n}} \tag{12.6.4}$$

as $n \to \infty$.

Theorem 2.10.1 has established the existence of the limit

$$A := \lim_{n\to\infty} \frac{n!}{n^{n+1/2}e^{-n}}. \tag{12.6.5}$$

The asymptotic behavior of the central binomial coefficients (12.6.4) provides the value of A.

Exercise 12.6.4. Use (12.6.4) to confirm the value $A = \sqrt{2\pi}$.

This completes the proof of **Stirling's formula**

$$n! \sim \sqrt{2\pi n}\, n^n e^{-n}. \tag{12.6.6}$$

Exercise 12.6.5. This exercise is a companion of Exercise 11.7.12. Define the sequence

$$v_n = v_{n-2} + \frac{1}{n-2} v_{n-1} \quad \text{for } n \geq 3 \tag{12.6.7}$$

with initial conditions $v_1 = 0$ and $v_2 = 1$. Prove that the generating function $V(x) = \sum_{n=1}^{\infty} v_n x^n$ satisfies $x(1-x)(1+x)V'(x) = (x+2)V(x)$. Its solution is given by

$$V(x) = \frac{x^2}{(1-x^2)} \sqrt{\frac{1+x}{1-x}}.$$

Then check that

$$\int_0^x \frac{V(t)}{t^2}\, dt = \sqrt{\frac{1+x}{1-x}} - 1.$$

Use the generating function for central binomial coefficients, given in Theorem 2.7.3, to obtain $v_{2n} = v_{2n+1} = nc_n/2^{2n-1}$. Use (12.6.4) to conclude that

$$\lim_{n\to\infty} \frac{2n}{v_n^2} = \pi. \tag{12.6.8}$$

12.7. The continued fraction of π

The material in Subsection 1.8.3 began with the decimal expansion of π:

$$\pi = 3.14159265358979932385\ldots$$

and produced, by truncation, rational approximations to π. For instance, the fraction

$$\alpha = \frac{78539823}{25000000} \sim 3.14159292000$$

satisfies $|\pi - \alpha| < 2.664 \times 10^{-7}$. On the other hand, the fraction $\beta = 355/113$ satisfies $|\pi - \beta| < 2.667 \times 10^{-7}$. It gives almost the same approximation to π but a smaller denominator. Note 1.9.31 explains the fact that among all fractions with denominator bounded by 113, the number

$$\beta = 3 + \cfrac{1}{7 + \cfrac{1}{15 + \cfrac{1}{1}}} = \frac{355}{113}$$

is the best approximation to π.

Now recall the procedure for the construction of the continued fraction for $x \in \mathbb{R}$. It will be employed to produce the first few convergents of π. (The name **convergents** is given the rational number

$$[x_0, x_1, \ldots, x_n] = \frac{p_n}{q_n}$$

that approximate x.) The continued fraction of x has the form

$$x = x_0 + \cfrac{1}{x_1 + \cfrac{1}{x_2 + \cfrac{1}{x_3 + \cfrac{1}{\cdots}}}}, \tag{12.7.1}$$

with $x_0 \in \mathbb{N}_0$ and $x_i \in \mathbb{N}$. It is clear that $x_0 = \lfloor x \rfloor$. The bounds in Exercise 12.2.4 show that $x_0(\pi) = 3$. To obtain the next integer x_1, observe that

$$\frac{1}{x - x_0} = x_1 + \cfrac{1}{x_2 + \cfrac{1}{x_3 + \cfrac{1}{x_4 + \cfrac{1}{\cdots}}}},$$

and, as before, it follows that

$$x_1 = \left\lfloor \frac{1}{x - x_0} \right\rfloor. \tag{12.7.2}$$

To obtain the value of x_1, it is required to have an accurate expression for $1/(\pi - 3)$.

Exercise 12.7.1. Let $y_n = (3n+1)/n$. Check that y_n decreases to its limit 3. The initial value is $y_1 = 4$. Therefore there is a first index n such that $y_n < \pi$. Confirm that $n = 8$ and that this gives the bound

$$7 \leq \frac{1}{\pi - 3} < 8.$$

Conclude that the second partial quotient is $x_1 = 7$. The rational approximation is $[3, 7] = 22/7$. The error term is guaranteed to be

$$|\pi - 22/7| < 1/(2 \cdot 7^2) = 1/98 \sim 0.0102041.$$

In fact, $|\pi - 22/7| < 0.00127$.

An algorithm for computing the continued fraction of $x \in \mathbb{R}$ is given in the next exercise.

Exercise 12.7.2. Define the double sequence $\{a_n, b_n\}$ by

$$a_n = \frac{1}{(a_{n-1} - b_{n-1})}, \qquad b_n = \lfloor a_n \rfloor$$

for $n \geq 1$, with initial conditions $a_0 = x$ and $b_0 = \lfloor a_0 \rfloor$. Prove that b_n is the nth partial quotient of the continued fraction of x, that is,

$$x = [b_0, b_1, b_2, b_3, \ldots] = b_0 + \cfrac{1}{b_1 + \cfrac{1}{b_2 + \cfrac{1}{b_3 + \cfrac{1}{\cdots}}}}.$$

Exercise 12.7.3. Define a `Mathematica` function that constructs the sequence $\{a_n,\, b_n\}$. Use it to evaluate the first terms of the continued fraction of π as

$$[3,\ 7,\ 15,\ 1,\ 292,\ 1,\ 1,\ 1,\ 2,\ 1,\ 3,\ 1,\ 14,\ 2,\ 1,\ 1, \ldots].$$

Compute the first five convergents as

$$\left\{3,\ \frac{22}{7},\ \frac{333}{106},\ \frac{355}{113},\ \frac{103993}{33102}\right\}$$

with corresponding error terms

$$\left\{0.1415,\ 0.00126,\ 8.321 \times 10^{-5},\ 2.667 \times 10^{-7},\ 5.778 \times 10^{-10}\right\}.$$

Observe the appearance of the convergents in the integrals given in Exercise 1.8.25.

The continued fraction in (12.7.1) is called **simple**. In the case of π, there are no apparent patterns for the partial quotients. E. W. Weisstein [**309**] has the current record for their computation, with 5821569425 partial quotients computed. (The date in [**309**] is recorded as September 18, 2011.) There are other types of continued fraction representations for real numbers closely related to π, where the patterns are predictable. An early example of a formula for π as well as a recent one are presented next.

12.7.1. The continued fractions of Lord Brouckner and L. J. Lange. One of the first recorded infinite continued fraction is

$$\frac{4}{\pi} = 1 + \cfrac{1^2}{2 + \cfrac{3^2}{2 + \cfrac{5^2}{2 + \cfrac{7^2}{2 + \cdots}}}}.$$

This was given by Lord Brouckner, the first president of the Royal Society of London, around 1659. The second example appeared in 1999 by L. J. Lange [**194**]. It states that

$$\pi = 3 + \cfrac{1^2}{6 + \cfrac{3^2}{6 + \cfrac{5^2}{6 + \cfrac{7^2}{6 + \cdots}}}}.$$

This section is dedicated to these two examples.

Lord Brouckner's example. The argument presented here is due to L. Euler. The author wishes to thank T. J. Osler for showing him the presentation in the paper by T. J. Osler [**239**]. Start with the Leibnitz series

$$\frac{\pi}{4} = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \cdots$$

given in Exercise 12.4.3. Write it in the form

$$\frac{\pi}{4} = 1 - \alpha_1,$$

with $\alpha_1 = 1/3 - 1/5 + 1/7 - 1/9 + \cdots$. Then

$$\frac{4}{\pi} = \frac{1}{1-\alpha_1} = 1 + \cfrac{1}{\cfrac{1-\alpha_1}{\alpha_1}} = 1 + \cfrac{1}{-1 + \cfrac{1}{\alpha_1}}.$$

Now write

$$\alpha_1 = \frac{1}{3} - \alpha_2,$$

with $\alpha_2 = 1/5 - 1/7 + 1/9 - 1/11 + \cdots$. Then

$$\frac{1}{\alpha_1} = \cfrac{1}{\cfrac{1}{3} - \alpha_2} = 3 + \cfrac{9}{-3 + \cfrac{1}{\alpha_2}}.$$

This gives

$$\frac{4}{\pi} = 1 + \cfrac{1}{2 + \cfrac{3^2}{-3 + \cfrac{1}{\alpha_2}}}.$$

Exercise 12.7.4. Complete the proof by an inductive argument.

L. J. Lange's example. The argument presented here is due to D. Bowman and it appeared at the end of the paper by L. J. Lange [**194**]. The first exercise evaluates a series by appealing to integration.

Exercise 12.7.5. Show that

$$\sum_{k=1}^{\infty} \frac{(-1)^{k-1}}{2k(2k+1)(2k+2)} = \frac{\pi - 3}{4}.$$

Hint: Integrate the identity

$$\sum_{k=0}^{\infty} (-1)^k x^k = \frac{1}{1+x}$$

from 0 to x and replace x by x^2 to produce

$$\sum_{k=1}^{\infty} \frac{(-1)^{k-1}}{2k} x^{2k} = \frac{\ln(1+x^2)}{2}.$$

Integrate two more times and use

$$\int_0^x \ln(1+t^2)\,dt = -2x + 2\arctan x + x\ln(1+x^2),$$

and integrate by parts to produce

$$\int_0^x \left(-2t + 2 \text{ arctan } t + t\ln(1+t^2)\right)\, dt$$
$$= -\frac{3}{2}x^2 + 2x \text{ arctan } x - \frac{1}{2}\ln(1+x^2) + \frac{1}{2}x^2\ln(1+x^2).$$

This gives the result.

Alternative hint: Expand the summand of the original series in partial fractions.

The next exercise verifies the identity of an alternating series and an infinite continued fraction.

Exercise 12.7.6. Let $a_k \neq 0$ be real numbers. Verify the identity

$$\sum_{k=1}^{\infty} \frac{(-1)^{k-1}}{a_k} = \cfrac{1}{a_1 + \cfrac{a_1^2}{a_2 - a_1 + \cfrac{a_2^2}{a_3 - a_2 + \cfrac{a_3^2}{a_4 - a_3 + \cdots}}}}.$$

The choice of $a_k = 2k(2k+1)(2k+2)$ gives Lange's continued fraction. **Hint:** Check that the partial sums and the convergents match.

12.8. The digits of π in base 16

The discovery of a formula that provides a fast computation of the binary digits of $\ln 2$ described in Section 11.9 led the authors of [**37**] to search for a similar expression for π. Their result is given in the next theorem. It is remarkable that this was not known before. In particular, how did Euler miss this?

Theorem 12.8.1. *The formula*

$$\pi = \sum_{k=0}^{\infty} \frac{1}{16^k}\left(\frac{4}{8k+1} - \frac{2}{8k+4} - \frac{1}{8k+5} - \frac{1}{8k+6}\right)$$

holds.

Proof. The proof of this formula is based on the evaluation

$$\int_0^{1/\sqrt{2}} \frac{x^{k-1}\,dx}{1-x^8} = \int_0^{1/\sqrt{2}} \sum_{j=0}^{\infty} x^{k-1+8j}\,dx = \frac{1}{2^{k/2}} \sum_{j=0}^{\infty} \frac{1}{16^j(8j+k)}.$$

Let S be the series in the statement of the theorem. Then

$$\begin{aligned} S &= \int_0^{1/\sqrt{2}} \frac{4\sqrt{2} - 8x^3 - 4\sqrt{2}x^4 - 8x^5}{1-x^8}\,dx \\ &= \int_0^1 \frac{16y-16}{y^4-2y^3+4y-4}\,dy, \end{aligned}$$

after the change of variables $y = \sqrt{2}x$. The partial fraction decomposition

$$\frac{16y-16}{y^4-2y^3+4y-4} = \frac{4y}{y^2-2} - \frac{4y-8}{y^2-2y+2}$$

gives the result. □

The result of the theorem yields an algorithm for the computation of the digits of π in base 16. It permits us to evaluate the hexadecimal digits of π beginning at an arbitrary starting position, without needing to calculate any of the preceding digits. ***No such algorithm is known for the decimal digits of*** π. In the article by D. H. Bailey, J. Borwein, A. Mattingly, and G. Wightwick [**33**], the authors discuss these methods for π^2 and other related constants. It has been conjectured that there is no BBP-formula (for Bailey-Borwein-Plouffe) for e. ***Only time will tell.***

12.9. Special values of trigonometric functions

Given a special function, it is always an interesting question to consider values in its domain that produce simpler outputs. In the trigonometric setting, the question is, *what angles θ have the property for which $\cos\theta$ is expressible by radicals*? This is motivated by the elementary examples

$$\cos\frac{\pi}{6} = \frac{\sqrt{3}}{2}, \quad \cos\frac{\pi}{4} = \frac{\sqrt{2}}{2}, \quad \cos\frac{\pi}{3} = \frac{1}{2}, \quad \text{and} \quad \cos\frac{\pi}{2} = 0.$$

Less well-known examples include

$$\cos\frac{\pi}{5} = \frac{\sqrt{5}+1}{4} \quad \text{and} \quad \cos\frac{\pi}{10} = \frac{\sqrt{5+\sqrt{5}}}{2\sqrt{2}}.$$

Naturally, this suggests considering the values

$$c_{n,m} = \cos\frac{\pi n}{m} \quad \text{and} \quad s_{n,m} = \sin\frac{\pi n}{m}. \tag{12.9.1}$$

Definition 12.9.1. A real number x is **expressible by radicals** if x can be obtained by a **finite** combination of the four basic operations of $\mathbb{R}$ (addition, subtraction, multiplication, and division) and the radical functions $f(x) = x^{1/n}$ $(n \in \mathbb{N})$ applied to integer values.

Example 12.9.2. The numbers

$$x_1 = \sqrt{2} + \sqrt{5} \quad \text{and} \quad x_2 = 2 + \sqrt{2} + \sqrt[3]{2+\sqrt{3}}$$

are expressible by radicals.

Definition 12.9.3. A number $a \in \mathbb{C}$ is called an **algebraic number** if there is a polynomial $P(x)$ with integer coefficients such that $x = a$ is a root of $P(x) = 0$. The **degree of** a is the minimal degree among all such polynomials.

Exercise 12.9.4. Let α be an algebraic number. Prove that the polynomial of minimal degree such that $P(\alpha) = 0$ is unique up to a constant. This constant may be normalized by assuming that the coefficients of P are relatively prime. It will be denoted by $\mathrm{Irr}(x, \alpha)$ and it is called the **minimal polynomial** of α.

Note 12.9.5. It turns out that every real number that is expressible by radicals is automatically algebraic. This is easy to see in the case of x_1 above. Indeed, write

$$x_1 - \sqrt{2} = \sqrt{5}$$

and square to produce

$$x_1^2 - 3 = 2\sqrt{2}x.$$

Squaring again shows that x_1 solves $P_1(x) = x^4 - 14x^2 + 9 = 0$. On the other hand, the number x_2 in Example 12.9.2 is a root of the polynomial

$$\begin{aligned}P_2(x) = x^{12} - 24x^{11} + 252x^{10} - 1528x^9 + 5964x^8 - 15936x^7\\ + 30770x^6 - 45720x^5 + 54660x^4 - 50600x^3 + 32424x^2\\ - 13296x + 3217.\end{aligned}$$

This polynomial was found by using the command

$$\texttt{MinimalPolynomial}[x_2]$$

in `Mathematica`.

The next result is elementary.

Theorem 12.9.6. *For any $n,\, m \in \mathbb{N}$, the values $c_{n,m}$ and $s_{n,m}$ in* (12.9.1) *are algebraic numbers.*

Proof. The polynomial R_m in Corollary 12.5.4 yields

$$R_m(c_{n,m}) = \cos(\pi n) = (-1)^n. \tag{12.9.2}$$

This shows that $c_{n,m}$ is algebraic. The proof for $s_{n,m}$ is similar. □

Example 12.9.7. The number $c_{1,5} = \cos(\pi/5)$ is algebraic because $R_5(c_{1,5}) = -1$. Define $P_5(x) = R_5(x) + 1$. The recurrences (12.5.5) yield

$$P_5(x) = (x+1)(x^2 - 2x - 1)^2.$$

It follows that $c_{1,5}$ is a root of the quadratic equation $4x^2 - 2x - 1 = 0$. Therefore

$$\cos\frac{\pi}{5} = \frac{\sqrt{5}+1}{4}.$$

Exercise 12.9.8. Verify the value

$$\cos\frac{\pi}{10} = \frac{\sqrt{5+\sqrt{5}}}{2\sqrt{2}}.$$

Example 12.9.9. The same analysis is now described for the number $c_{1,7} = \cos(\pi/7)$. Define $P_7(x) = R_7(x) + 1$. Then $P_7(c_{1,7}) = 0$, showing that $c_{1,7}$ is algebraic. The recurrences (12.5.5) show that

$$P_7(x) = 64x^7 - 112x^5 + 56x^3 - 7x + 1 = (x+1)(8x^3 - 4x^2 - 4x + 1)^2.$$

The fact that $\cos\frac{\pi}{7} \neq -1$ shows that this number is a root of the polynomial

$$T(x) = 8x^3 - 4x^2 - 4x + 1. \tag{12.9.3}$$

Exercise 12.9.10. Give a direct proof of the statement in Example 12.9.9 using

$$\frac{\pi}{7}+\frac{2\pi}{7}=\pi-\frac{4\pi}{7}$$

and the addition theorem for trigonometric functions.

The irreducibilty of T was established in Example 4.6.2 using the criteria for rational roots of a polynomial. The next theorem gives another criteria for the irreducibility of a polynomial. It is then used to verify again that T is irreducible. This shows that $\cos \pi/7$ is an algebraic number of degree 3.

Theorem 12.9.11 (Eisenstein's irreducibilty criteria). *Let*

$$A(x)=a_n x^n+a_{n-1}x^{n-1}+\cdots+a_1 x+a_0 \tag{12.9.4}$$

be a polynomial with integer coefficients and $\gcd(a_n,\, a_{n-1},\, \ldots, a_0)=1$. *Assume there is a prime* p *such that* p *divides* a_i *for* $0 \le i < n$, p *does not divide* a_n, *and* p^2 *does not divide* a_0. *Then* $A(x)$ *is irreducible over* $\mathbb{Z}$.

Proof. Assume A factors in the form

$$A(x)=(b_r x^r+b_{r-1}x^{r-1}+\cdots+b_0)(c_s x^s+c_{s-1}x^{s-1}+\cdots+c_0)$$

with $b_i,\, c_j \in \mathbb{Z}$. Comparing the constant terms gives $a_0=b_0c_0$. It follows that p divides only one of b_0 and c_0 because p divides a_0 and p^2 does not. Assume p divides b_0. Now suppose p divides $b_0,\, b_1,\, \ldots, b_{i-1}$ and p does not divide b_i. Comparing the coefficients of x^i gives

$$a_i=b_ic_0+b_{i-1}c_1+\cdots$$

and the divisibility assumptions show that p divides b_ic_0. This is impossible. It follows that p divides all the coefficients b_i. This implies that p divides a_n. This contradiction shows that A is irreducible. □

The next exercise checks that the polynomial $T(x)$ defined in (12.9.3) is irreducible. Therefore $T(x)=\operatorname{Irr}(\cos \pi/7, x)$ and $\cos \pi/7$ is an algebraic number of degree 3. The discussion for $c_{n,m}$ and $s_{n,m}$ is postponed until Chapter 14.

Exercise 12.9.12. Prove that $T(x)$ is irreducible. **Hint:** Consider the polynomial

$$S(x) = (x-1)^3\, T\left(\frac{1}{x-1}\right).$$

12.10. The roots of a cubic polynomial

It is natural to expect that an expression for $\cos(\pi/7)$ in radicals may be obtained by using the formulas for solving cubic equations described in Chapter 4. The goal of this section is to describe in detail the computation of the roots of the polynomial

$$T(x) = 8x^3 - 4x^2 - 4x + 1$$

satisfied by $\cos \pi/7$ and then suggest an alternative form of the computation of the roots of any cubic.

Exercise 12.10.1. Check that $T(x) = 0$ has three real roots.

The first step in the computation of the roots of T is to convert it to its reduced form. Define $T_1(x) = T(x + 1/6)$ and check that

$$T_1(x) = 8x^3 - \frac{14}{3}x + \frac{7}{27}.$$

Dividing by the leading coefficient yields the reduced form

$$T_2(x) = x^3 - \frac{7}{12}x + \frac{7}{216}.$$

Exercise 12.10.2. Check that the discriminant of the reduced form is $D = -7^2/(3 \cdot 48^2)$. Use Theorem 4.7.12 to confirm that $T(x) = 0$ has three distinct real roots.

The next step is to compute the functions $s(a, b)$ and $t(a, b)$ given in Theorem 4.6.8 as

$$s(a,b) = \left(\frac{b}{2} + \sqrt{D}\right)^{1/3} \quad \text{and} \quad t(a,b) = \left(\frac{b}{2} - \sqrt{D}\right)^{1/3}.$$

For $a = -7/12$ and $b = 7/216$, this gives

$$s\left(-\frac{7}{12}, \frac{7}{216}\right) = \left(\frac{7}{432} + \frac{7i}{48\sqrt{3}}\right)^{1/3}$$

and

$$t\left(-\frac{7}{12},\frac{7}{216}\right)=\left(\frac{7}{432}-\frac{7i}{48\sqrt{3}}\right)^{1/3}.$$

Exercise 12.10.3. Convert the complex numbers above to polar coordinates and check that

$$s\left(-\frac{7}{12},\frac{7}{216}\right)=\frac{\sqrt{7}}{6}\left[\cos\left(\frac{\tan^{-1}(3\sqrt{3})}{3}\right)+i\sin\left(\frac{\tan^{-1}(3\sqrt{3})}{3}\right)\right],$$
$$t\left(-\frac{7}{12},\frac{7}{216}\right)=\frac{\sqrt{7}}{6}\left[\cos\left(\frac{\tan^{-1}(3\sqrt{3})}{3}\right)-i\sin\left(\frac{\tan^{-1}(3\sqrt{3})}{3}\right)\right].$$

In conclusion. The roots of the polynomial equation $T(x)=0$, one of which is $\cos(\pi/7)$, are given in terms of the angle $\alpha=\frac{1}{3}\tan^{-1}(3\sqrt{3})$ by

$$\begin{aligned}x_1 &= \frac{1}{6}-\frac{\sqrt{7}}{3}\cos\alpha,\\ x_2 &= \frac{1}{6}+\frac{\sqrt{7}}{6}\cos\alpha+\frac{\sqrt{7}}{2\sqrt{3}}\sin\alpha,\\ x_3 &= \frac{1}{6}+\frac{\sqrt{7}}{6}\cos\alpha-\frac{\sqrt{7}}{2\sqrt{3}}\sin\alpha.\end{aligned}$$

Computing a numerical approximation to these roots shows that x_2 is the root $\cos(\pi/7)$. This gives the remarkably complicated-looking trigonometric identity

$$\cos\frac{\pi}{7}=\frac{1}{6}+\frac{\sqrt{7}}{6}\cos\left(\frac{\tan^{-1}3\sqrt{3}}{3}\right)+\frac{\sqrt{7}}{2\sqrt{3}}\sin\left(\frac{\tan^{-1}3\sqrt{3}}{3}\right).$$

Exercise 12.10.4. Try to check it. Do not spend too much time on it.

Note 12.10.5. The formula for x_2 is not the answer to the question of expressing $\cos(\pi/7)$ in radicals. The answer is the remarkable theorem of Gauss which states that the trigonometric function of the angle π/N can be expressed in terms of square roots if and only if N has the form $N=2^k\cdot f_0f_1\cdots f_n$ where the f_j are distinct **Fermat primes**. These are primes of the form 2^m+1 (it is a corollary that m has to be a power of 2) and have appeared in Note 1.7.10. There are ony five known cases:

$$f_0 = 3, \quad f_1 = 5, \quad f_2 = 17, \quad f_3 = 257, \quad f_4 = 65537.$$

In particular, $N = 7$ is not of this form. Therefore $\cos(\pi/7)$ cannot be expressed by radicals.

The trigonometric method for solving cubics. This section considers the solution of the cubic polynomial equation

$$P_3(x) = a_0x^3 + a_1x^2 + a_2x + a_3 = 0$$

by using trigonometric functions. This method differs from that of Cardano given in Chapter 4. The comments at the end of the section show that this method generalizes to produce formulas for the solution of any polynomial equation.

The first step is to normalize the equation. The choice of normalization is motivated by the identity given in the next exercise.

Exercise 12.10.6. Use the addition theorem to prove

$$\sin 3x = -4\sin^3 x + 3\sin x. \tag{12.10.1}$$

Exercise 12.10.7. Prove that every cubic equation $P_3(x) = 0$ can be converted to the form

$$N_3(t) = 4t^3 - 3t + c = 0 \tag{12.10.2}$$

by scaling and square root extraction. **Hint:** Transform the equation $P_3(x) = 0$ by the following steps.

- First scale it to the form

$$P(x) = 4x^3 + \frac{4a_1}{a_0}x^2 + \frac{4a_2}{a_0}x + \frac{4a_3}{a_0} = 0$$

and then, to eliminate the term in x^2, define

$$M(x) = P\left(x - \frac{a_1}{3a_0}\right).$$

Check that $M(x)$ has the form $M(x) = 4x^3 + b_2x + b_3$, with

$$\begin{aligned} b_2(a_0, a_1, a_2, a_3) &= \frac{4(3a_0a_2 - a_1^2)}{3a_0^2}, \\ b_3(a_0, a_1, a_2, a_3) &= \frac{4(2a_1^3 - 9a_0a_1a_2 + 27a_0^2a_3)}{27a_0^3}. \end{aligned}$$

- The next step is to let $x = \lambda t$, with $\lambda = \sqrt{-b_2/3}$, to convert $M(x) = 0$ to (12.10.2), with

$$c = \frac{3\sqrt{3}b_3}{\sqrt{-b_2^3}}. \tag{12.10.3}$$

Definition 12.10.8. This normalization of $P_3(x) = 0$ to $N_3(t) = 0$ is called the **trigonometric form** of the cubic.

The solution to the cubic equation $N_3(t) = 0$ is now clear: choose an angle ϑ_1 such that $\sin(3\vartheta_1) = c$. Observe that, once ϑ_1 is chosen, the values $\vartheta_2 := \vartheta_1 + \frac{2\pi}{3}$ and $\vartheta_3 := \vartheta_2 + \frac{4\pi}{3}$ also satisfy

$$\sin(3\vartheta_2) = \sin(3\vartheta_3) = c. \tag{12.10.4}$$

Exercise 12.10.6 now shows that the roots of $N_3(t) = 0$ are

$$t_1 = \sin\vartheta_1, \quad t_2 = \sin\vartheta_2, \quad t_3 = \sin\vartheta_3. \tag{12.10.5}$$

Example 12.10.9. Consider the polynomial $P(x) = 8x^3 + 72x^2 + 210x + 199$. The first step in finding its roots is to reduce it to its trigonometric form. The coefficient of x^2 is eliminated by the shift $t = x - 3$. Then

$$P_1(t) := P(t-3) = 8t^3 - 6t + 1. \tag{12.10.6}$$

Then dividing by 2 yields the normalization

$$N_3(t) = 4t^3 - 3t + \tfrac{1}{2}. \tag{12.10.7}$$

To find the roots of $N(t)$, choose an angle ϑ_1 so that

$$\sin(3\vartheta_1) = \tfrac{1}{2}, \tag{12.10.8}$$

for instance $\vartheta_1 = \frac{\pi}{18}$. The associated angles are now $\vartheta_2 = \frac{13\pi}{18}$ and $\vartheta_3 = \frac{25\pi}{18}$. The roots of the cubic equation $8x^3+72x^2+210x+199 = 0$ are

$$x_1 = 3 + \sin\frac{\pi}{18}, \quad x_2 = 3 + \sin\frac{13\pi}{18}, \quad x_1 = 3 + \sin\frac{25\pi}{18}. \tag{12.10.9}$$

Exercise 12.10.10. Sometimes the numbers do not come out so clean. Check that the trigonometric form of

$$P_3(x) = 154x^3 + 31x^2 - 36x - 9 = 0$$

is

$$N_3(t) = 4t^3 - 3t^2 - \frac{2078315}{(17593)^{3/2}} = 0.$$

Exercise 12.10.11. Use the trigonometric form of the cubic to show that the roots of $64x^3 - 192x^2 - 60x - 1 = 0$ are given by

$$\frac{\cos^3(a)}{\cos(3a)}, \quad \frac{\cos^3(2a)}{\cos a}, \quad \frac{\cos^3(3a)}{\cos(2a)},$$

with $a = 2\pi/7$.

Exercise 12.10.12. This exercise deals with the polynomial

$$T(x) = 8x^3 - 4x^2 - 4x + 1$$

that appeared in the discussion related to $\cos(\pi/7)$. Check that the trigonometric form of this equation is given by

$$N(t) = 4t^3 - 3t + \frac{1}{2\sqrt{7}}.$$

Evaluate the roots in the form

$$\begin{aligned} x_1 &= \frac{1}{6} + \frac{\sqrt{7}}{3}\sin\theta, \\ x_2 &= \frac{1}{6} + \frac{\sqrt{7}}{3}\sin\left(\theta + 2\pi/3\right), \\ x_3 &= \frac{1}{6} + \frac{\sqrt{7}}{3}\sin\left(\theta + 4\pi/3\right), \end{aligned}$$

with

$$\theta = \frac{1}{3}\sin^{-1}\left(\frac{1}{2\sqrt{7}}\right).$$

Use these roots to obtain a second trigonometric identity:

$$\cos\frac{\pi}{7} = \frac{1}{6} + \frac{\sqrt{7}}{3}\sin\left[\frac{2\pi}{3} + \frac{1}{3}\sin^{-1}\left(\frac{1}{2\sqrt{7}}\right)\right].$$

Compare this with the expression considered in Exercise 12.10.4.

12.11. A special trigonometric integral

The evaluation of integrals in closed form is considered by many researchers an **art form**. There is no developed algorithm that will reduce this question to a finite set of rules. The classical examples

$$\int_0^{\pi/2} \cos^{2n} x\, dx = \frac{1}{2^{2n}}\binom{2n}{n}\frac{\pi}{2}$$

and

$$\int_0^{\pi/2} \cos^{2n+1} x\, dx = \frac{2^{2n}}{(2n+1)\binom{2n}{n}},$$

given as Exercise 12.6.2, illustrate the evaluation of integrals by producing recurrences for them. The reader is referred to the classical text by J. Edwards [**117, 118**] for a nice collection of methods for the evaluation of definite integrals. Many of these evaluations have been collected in tables of integrals such as those by A. Apelblat [**24**], Y. A. Brychkov [**84**], the classical table by I. S. Gradshteyn and I. M. Ryzhik [**144**], and the five-volume compendium by A. P. Prudnikov, Yu. A. Brychkov, and O. I. Marichev [**250**]. The current author has begun a program dedicated to the evaluation of all entries in [**144**]. The papers [**11, 13, 14, 222**] contain some examples involving trigonometric functions. **The reader is now officially invited to help.**

This section describes the evaluation of a sequence of integrals where the integrand is the power of the function $\frac{\sin x}{x}$.

Example 12.11.1. The first example deals with the evaluation of

$$\int_0^{\infty} \frac{\sin x}{x}\, dx = \frac{\pi}{2}. \tag{12.11.1}$$

The simplest proof (to anyone familiar with the classical text by J. Edwards [**117**]) is to introduce a damping factor and to consider

$$f(t) = \int_0^{\infty} e^{-tx} \frac{\sin x}{x}\, dx. \tag{12.11.2}$$

Differentiating yields

$$f'(t) = -\int_0^{\infty} e^{-tx} \sin x\, dx. \tag{12.11.3}$$

Integration by parts (twice) gives

$$f'(t) = -\frac{1}{1+t^2}. \tag{12.11.4}$$

Evaluate the constant of integration by letting $t \to \infty$ to obtain $f(t) = \pi/2 - \tan^{-1} t$. The original integral is simply $f(0)$.

Example 12.11.2. The value of

$$\int_0^\infty \left(\frac{\sin x}{x} \right)^2 dx = \frac{\pi}{2} \tag{12.11.5}$$

can be obtain by the same method. Define

$$f(t) = \int_0^\infty e^{-tx} \left(\frac{\sin x}{x} \right)^2 dx \tag{12.11.6}$$

and observe that

$$f''(t) = \int_0^\infty e^{-tx^2} \sin^2 x \, dx. \tag{12.11.7}$$

This integral can be evaluated by writing $\sin^2 x = \frac{1}{2}(1 - \cos 2x)$ and integrating by parts. As an alternative, the `Mathematica` command

```
Integrate[Exp(-tx)(Sin[x])^2,{x,0,Infinity},Assumptions(t>0)]
```

gives the result

$$f''(t) = \frac{2}{t(t^2+4)}. \tag{12.11.8}$$

Integrate twice to obtain

$$f(t) = -\tan^{-1}\frac{t}{2} + \frac{1}{2}t \, \ln t - \frac{1}{4} t \ln(t^2+4) + \frac{\pi}{2}, \tag{12.11.9}$$

where the constant of integration comes from the condition $f(t) \to 0$ as $t \to \infty$. The value of the integral is then computed from $f(0)$.

The general case is given in the next theorem.

Theorem 12.11.3. *Define*

$$I_n = \int_0^\infty \left(\frac{\sin x}{x} \right)^n dx.$$

Then

$$I_n = \frac{\pi}{2^n (n-1)!} \sum_{j=0}^{\lfloor \frac{n-1}{2} \rfloor} (-1)^j \binom{n}{j} (n-2j)^{n-1}.$$

Proof. Introduce the auxiliary function

$$f_n(t) = \int_0^\infty e^{-xt} \left(\frac{\sin x}{x} \right)^n dx.$$

Then

$$J_n = J_n(t) := (-1)^n \left(\frac{d}{dt}\right)^n f_n(t) = \int_0^\infty e^{-xt}(\sin x)^n\, dx.$$

To evaluate J_n, integrate by parts to produce

$$J_n = \frac{n}{t}\int_0^\infty e^{-xt}(\sin x)^{n-1}\ \cos x\, dx$$

and one further integration by parts yields the recurrence

$$J_n = \frac{n}{t^2}\left[(n-1)J_{n-2} - nJ_n\right].$$

Therefore

$$J_n = \frac{n(n-1)}{n^2+t^2}J_{n-2}.$$

Iterating this recurrence and using the initial values

$$J_0 = \frac{1}{t} \quad \text{and} \quad J_1 = \frac{1}{1+t^2}$$

gives

$$J_n = \frac{n!}{t}\prod_{j=1}^{n/2}(t^2+(2j)^2)^{-1} \qquad \text{if } n \text{ is even}$$

and

$$J_n = n! \prod_{j=1}^{\frac{1}{2}(n+1)} (t^2+(2j-1)^2)^{-1} \qquad \text{if } n \text{ is odd.}$$

Exercise 12.11.4. Prove the identity

$$f_n(t) = \frac{(-1)^n}{(n-1)!}\int_t^\infty (s-t)^{n-1}\, J_n(s)\, ds.$$

It follows that

$$\int_0^\infty \left(\frac{\sin x}{x}\right)^n\ dx = f_n(0) = n\int_0^\infty s^{n-2}\prod_{j=1}^{n/2}(s^2+4j^2)^{-1}\, ds$$

if n is even and

$$\int_0^\infty \left(\frac{\sin x}{x}\right)^n\ dx = n\int_0^\infty s^{n-1}\prod_{j=1}^{\frac{1}{2}(n+1)}(s^2+(2j-1)^2)^{-1}\, ds$$

if n is odd.

The integral (12.11.3) is computed via a partial fraction decomposition of the integrand. Assume n is even, say $n = 2m$, and write $t = s^2$. Now look for an expansion of the form

$$\frac{2mt^{m-1}}{(t+4\cdot 1^2)(t+4\cdot 2^2)\cdots(t+4\cdot m^2)} = \sum_{r=1}^{m} \frac{A_r}{t+4r^2}.$$

The constants A_r are determined in the next exercise.

Exercise 12.11.5. Compute the value of A_{r_0} by multiplying the expansion by $(t+4r_0^2)$ and letting $t \to -4r_0^2$. Then simplify the expression for the integral to complete the proof in the case of n even.

The case of n odd is treated with the same procedure. The proof of Theorem 12.11.3 is complete. □

12.12. The infinite product for $\sin x$

This section contains a discussion of the product representations for trigonometric functions. These appeared in Euler's treatise [**122**] in 1748. The reader will find historical information about these topics in the book by P. Nahim [**231**], and the paper by W. Walter [**303**] has several approaches to this product.

Theorem 12.12.1. *The product representations for* $\sin x$ *and* $\cos x$ *are given by*

$$\sin x = x \prod_{k=1}^{\infty} \left(1 - \frac{x^2}{(\pi k)^2} \right) \tag{12.12.1}$$

and

$$\cos x = \prod_{k=1}^{\infty} \left(1 - \frac{x^2}{(\pi(k-\frac{1}{2}))^2} \right). \tag{12.12.2}$$

Proof. The argument given here appears in the paper by K. Venkatachaliengar [**297**]. Start with

$$I_n(x) := \int_0^{\pi/2} \cos xt \, \cos^n t \, dt$$

and integrate by parts to obtain $n(n-1)I_{n-2}(x) = (n^2 - x^2)I_n(x)$. Since $I_n(0) > 0$, it follows that, for $n \geq 2$,

$$\frac{I_{n-2}(x)}{I_{n-2}(0)} = \left(1 - \frac{x^2}{n^2}\right)\frac{I_n(x)}{I_n(0)}. \tag{12.12.3}$$

Using the values $I_0(0) = \pi/2$ and $I_1(0) = 1$, it follows that

$$\sin\left(\frac{\pi x}{2}\right) = \frac{\pi x}{2}\,\frac{I_0(x)}{I_0(0)} \quad \text{and} \quad \cos\left(\frac{\pi x}{2}\right) = (1 - x^2)\,\frac{I_1(x)}{I_1(0)}.$$

Now

$$\begin{aligned} |I_n(0) - I_n(x)| &= \left| \int_0^{\pi/2} (1 - \cos xt)\cos^n t\, dt \right| \\ &\leq \frac{1}{2}x^2 \int_0^{\pi/2} t^2 \cos^n t\, dt \\ &\leq \frac{1}{2}x^2 \int_0^{\pi/2} t \cos^{n-1} t\, \sin t\, dt \\ &= \frac{1}{n} I_n(0), \end{aligned}$$

where the inequality $t \leq \tan t$ has been employed. Thus

$$\lim_{n\to\infty} \frac{I_n(x)}{I_n(0)} = 1.$$

Now replace $\pi x/2$ by x to produce (12.12.1). □

Exercise 12.12.2. Use the recurrence (12.12.3) to obtain a closed form for the integral $I_n(x)$.

Exercise 12.12.3. Use (12.12.1) to derive **Wallis' infinite product** for π:

$$\pi = 2\prod_{k=1}^{\infty} \frac{2k}{2k-1}\cdot\frac{2k}{2k+1}.$$

This has appeared in (12.6.3).

Exercise 12.12.4. This exercise outlines a second proof of the product representation for $\sin x$ given in (12.12.1).

(a) Prove the identity

$$\sin(nx) \quad = \quad K(n)\sin x \times \prod_{r=1}^{(n-1)/2} \left(1 - \frac{\sin^2 x}{\sin^2(\pi r/n)} \right),$$

for n odd. **Hint:** Locate the zeros of $\sin(nx)$.

(b) Let $x \to 0$ to obtain $K(n) = n$.

(c) Conclude that

$$\sin x \quad = \quad n\sin(x/n) \prod_{r=1}^{\infty} \left(1 + f_r(n,x)\right), \tag{12.12.4}$$

where

$$f_r(n,x) \quad = \quad \begin{cases} 0 & r > (n-1)/2, \\ -\frac{\sin^2(x/n)}{\sin^2(r\pi/n)} & r \leq (n-1)/2. \end{cases} \tag{12.12.5}$$

(d) Let $n \to \infty$ to obtain (12.12.1). The representation (12.12.2) follows from the identity $\cos x = \sin(2x)/2\sin x$.

Note 12.12.5. J. Wästlund [**306**] describes an elementary proof of this product that is **free of integrals**.

Note 12.12.6. The convergence of an infinite product can be treated in parallel to that of infinite series. Given a sequence of positive numbers $\{a_n\}$, form the partial products

$$p_n = (1+a_1)(1+a_2)\cdots(1+a_n) \tag{12.12.6}$$

and if p_n converges to a limit p, then write

$$p = \prod_{n=1}^{\infty}(1+a_n). \tag{12.12.7}$$

It turns out that p_n converges if and only if the series $\sum a_n$ converges. See the textbook by O. Hijab [**168**] for details and examples.

Exercise 12.12.7. The convergence of the product and the series above it is proved by establishing elementary bounds. In general, there is no exact relation between the series and the product. Check the nice special case: if $a_n = 1/(4n^2 - 1)$, then

$$\prod_{n=1}^{\infty} (1 + a_n) = \pi \times \sum_{n=1}^{\infty} a_n.$$

Note 12.12.8. The factorization of a polynomial in terms of its roots, given in Exercise 4.4.9, cannot be extended directly to the case of a function with infinitely many roots. The construction of a function f with roots at $\{a_1, a_2, \ldots\}$ via

$$f(x) = \prod_{k=1}^{\infty} \left(1 - \frac{x}{a_k} \right) \tag{12.12.8}$$

might not be convergent. Weiestrass introduced **elementary factors**

$$\begin{aligned} E_0(z) &= 1 - z, \\ E_p(z) &= (1 - z) \exp \left(z + z^2/2 + \cdots + z^p/p \right) \end{aligned}$$

and showed that it is possible to choose indices p_k so that the modified product

$$P(x) = \prod_{k=1}^{\infty} E_{p_k} \left(\frac{z}{a_k} \right)$$

gives an honest function with the desired zeros. The book by R. Greene and S. Krantz [**148**] gives complete details.

12.13. The irrationality of π

An elementary proof due to I. Niven [**237**] of the irrationality of π is discussed next. The proof is based on the explicit construction of a family of polynomials whose derivatives take integer values at two points. The polynomials f_n are a scaled version of the Legendre polynomials described in Chapter 14.

Lemma 12.13.1. *Let $n \in \mathbb{N}$ and $a, b \in \mathbb{Z}$. The polynomial*

$$f_n(x) = \frac{1}{n!} x^n (a - bx)^n \tag{12.13.1}$$

has the property that f_n and all its derivatives at $x = 0$ and $x = a/b$ are integers.

Proof. The result is established at $x = 0$. The case of $x = a/b$ follows by symmetry. Expanding the binomial $(a - bx)^n$ gives

$$f_n^{(j)}(x) = \frac{1}{n!}\sum_{r=0}^{n}\binom{n}{r}(-1)^r a^{n-r} b^r (r+n)(r+n-1)\cdots(r+n-j+1)x^{r+n-j}.$$

This gives $f_n^{(j)}(0) = 0$ for $0 \leq j < n$ and $j > 2n$. The value $f_n^{(n)}(0) = a^n$ is also an integer. In the range $n < j \leq 2n$, the only term that does not vanish has index $r = j - n$. This gives

$$f_n^{(j)}(0) = \frac{j!}{n!}\binom{n}{j-n} a^{2n-j} b^j,$$

and this is also an integer. □

Theorem 12.13.2. *The number π is irrational.*

Proof. Suppose $\pi = a/b$, with a, $b \in \mathbb{N}$. Form the function

$$F(x) = f(x) - f^{(2)}(x) + f^{(4)}(x) - \cdots + (-1)^n f^{(2n)}(x)$$

and observe that

$$\frac{d}{dx}\left(F'(x)\sin x - F(x)\cos x\right) = \left(F''(x) + F(x)\right)\sin x.$$

Therefore

$$\int_0^{\pi} f(x)\sin x\,dx = F(\pi) + F(0) \in \mathbb{N}.$$

This is incompatible with the behavior

$$0 < f(x)\sin x < \frac{\pi^n a^n}{n!} \to 0 \qquad (12.13.2)$$

as $n \to \infty$. This contradiction shows that $\pi \notin \mathbb{Q}$. □

An extension due to A. E. Parks [**241**] is presented next.

Theorem 12.13.3. *Let $c \in \mathbb{R}^+$ and let f be a continuous function on $[0, c]$, positive on $(0, c)$. Suppose the antiderivatives f_1, $f_2, \ldots$ with $f_1' = f$ and $f_k' = f_{k-1}$ have the property that $f_k(0)$ and $f_k(c)$ are integers. Then c is irrational.*

Proof. Let $\mathfrak{P}$ be the class of polynomials $g(x)$ with real coefficients such that $g(0), g(c), g'(0), g'(c), \ldots, g^{(k)}(0), g^{(k)}(c), \ldots$ are all integers.

Exercise 12.13.4. Integrate by parts to prove that

$$\int_0^c f(x)g(x)\,dx \in \mathbb{Z}.$$

Assume now that $c = a/b \in \mathbb{Q}$. The class $\mathfrak{P}$ is closed under products and contains the polynomials $a - 2bx$ and $g_k(x) = x^k(a - bx)^k/k!$.

The bound

$$\int_0^c f(x)g_k(x)\,dx \geq 1 \tag{12.13.3}$$

follows from the fact that it is positive and an integer. Now let M be an upper bound for $x(a - bx)$ and let L be a bound for f on $[0, c]$. Then

$$\int_0^c f(x)g_k(x)\,dx \quad \leq \quad cL\frac{M^k}{k!} \tag{12.13.4}$$

converges to 0 as $n \to \infty$. This contradicts (12.13.3). □

Exercise 12.13.5. Let $r = m/n \in \mathbb{Q}$. Use the function $f(x) = ne^x$ to prove that $\ln r$ is not rational.

Note 12.13.6. Irrationality properties concerning π and related numbers are difficult to establish. It is (still) an open question to decide whether $\pi + e$ is irrational. The same is true for πe. The next theorem shows that one of them must be irrational.

Theorem 12.13.7. *One of the numbers $\pi + e$ or πe is irrational.*

Proof. Assume the conclusion is false. Then

$$P(x) = (x - e)(x - \pi) = x^2 - (\pi + e)x + \pi e \tag{12.13.5}$$

is a quadratic polynomial with rational coefficients and $P(e) = 0$. This contradicts Liouville's theorem, Theorem 11.5.2. □

The next theorem, established by C. L. F. Lindenmann in 1882, shows that π is a transcendental number. In particular, this shows that all powers π^n are irrational numbers. The reader will find the details in the notes by M. Filaseta [**126**] and the paper by I. Niven [**236**].

Theorem 12.13.8. *The number π is transcendental.*

12.14. Arctangent sums and a dynamical system

The evaluation of arctangent sums of the form

$$\sum_{k=1}^{\infty} \tan^{-1} h(k)$$

for a rational function h reappear in the literature from time to time. For instance the evaluation of

$$\sum_{k=1}^{\infty} \tan^{-1} \frac{2}{k^2} \quad = \quad \frac{3\pi}{4} \tag{12.14.1}$$

was proposed by J. Anglesio [**22**] in 1993. This is a classical problem that appears in the book by G. Chrystal [**101**], the paper by J. W. L. Glaisher [**138**], and the book by S. L. Loney [**203**], among other places. The evaluation of

$$\sum_{k=1}^{\infty} \tan^{-1} \frac{1}{k^2} = \tan^{-1} \frac{\tan(\pi/\sqrt{2}) - \tanh(\pi/\sqrt{2})}{\tan(\pi/\sqrt{2}) + \tanh(\pi/\sqrt{2})}$$

was proposed by R. J. Chapman [**96**] in 1990. This was solved by A. Sarkar [**267**] using a method that involves the zeros of polynomials. The reader will find details in the survey paper by G. Boros and V. Moll [**66**].

This section discusses the evaluation of these sums. Throughout, $\tan^{-1} x$ will always denote the principal value. The addition formulas for $\tan^{-1} x$ are employed throughout:

$$\tan^{-1} x + \tan^{-1} y \quad = \quad \begin{cases} \tan^{-1} \frac{x+y}{1-xy} & \text{if } xy < 1, \\ \tan^{-1} \frac{x+y}{1-xy} + \pi \text{ sign } x & \text{if } xy > 1 \end{cases}$$

and

$$\tan^{-1} x + \tan^{-1} \frac{1}{x} = \frac{\pi}{2} \text{ sign } x.$$

Exercise 12.14.1. The addition formula for arctangents has some peculiar consequences. Here is an instance. Let F_n be the nth Fibonacci number. Check that

$$\tan^{-1}\left(\frac{1}{F_{2n}}\right) = \tan^{-1}\left(\frac{1}{F_{2n+1}}\right) + \tan^{-1}\left(\frac{1}{F_{2n+2}}\right).$$

Iterate this relation to obtain

$$\tan^{-1}\left(\frac{1}{F_{2n}}\right) = \sum_{k=n}^{\infty} \tan^{-1}\left(\frac{1}{F_{2k+1}}\right)$$

and

$$\frac{\pi}{4} = \sum_{k=1}^{\infty} \tan^{-1}\left(\frac{1}{F_{2k+1}}\right).$$

Compute the error after taking 100 terms in the series.

The method of telescoping. The evaluation of sums in telescoping form is elementary. Cancellation leads immediately to

$$\sum_{k=1}^{n} a_{k+1} - a_k = a_{n+1} - a_1. \tag{12.14.2}$$

Theorem 12.14.2. *Let f be of fixed sign and define h by*

$$h(x) = \frac{f(x+1) - f(x)}{1 + f(x+1)f(x)}. \tag{12.14.3}$$

Then

$$\sum_{k=1}^{n} \tan^{-1} h(k) = \tan^{-1} f(n+1) - \tan^{-1} f(1). \tag{12.14.4}$$

In particular, if f has a limit at ∞ (including the possibility of $f(\infty) = \infty$), then

$$\sum_{k=1}^{\infty} \tan^{-1} h(k) = \tan^{-1} f(\infty) - \tan^{-1} f(1). \tag{12.14.5}$$

Proof. Since

$$\tan^{-1} h(k) = \tan^{-1} f(k+1) - \tan^{-1} f(k),$$

the result follows by telescoping. □

Exercise 12.14.3. Take $f(x) = ax + b$, where a and b are such that $f(x) \geq 0$ for $x \geq 1$. Use Theorem 12.14.2 to show that the special case of $a = 1$, $b = 0$ gives the sum

$$\sum_{k=1}^{\infty} \tan^{-1} \frac{1}{k^2 + k + 1} = \frac{\pi}{4}$$

and $a = 2$, $b = 0$ gives

$$\sum_{k=0}^{\infty} \tan^{-1} \frac{2}{(2k+1)^2} = \frac{\pi}{2}.$$

Exercise 12.14.4. Prove that

$$\sum_{k=1}^{\infty} \tan^{-1} \frac{2}{k^2} = \frac{3\pi}{4}.$$

This problem was proposed by J. Anglesio [**22**].

Exercise 12.14.5. Prove that

$$\sum_{k=1}^{\infty} \tan^{-1} \frac{4ak}{k^4 + a^2 + 4} = \tan^{-1} \frac{a}{2} + \tan^{-1} a.$$

Compute the special value $a = 1$.

A dynamical system. An interesting dynamical system involving arctangent sums appeared from the addition theorem. In order to present the problem, define

$$x_n = \tan \sum_{k=1}^{n} \tan^{-1} k. \tag{12.14.6}$$

Then $x_1 = 1$ and the addition theorem for arctangent gives

$$x_n = \frac{x_{n-1} + n}{1 - n x_{n-1}}. \tag{12.14.7}$$

The evolution of the sequence $\{x_n : n \in \mathbb{N}\}$ is a discrete dynamical system with many interesting questions. The list of the first few values, starting with $x_1 = 1$, is

$$\left\{ 1, \, -3, \, 0, \, 4, \, -\frac{9}{19}, \, \frac{105}{73}, \, -\frac{308}{331}, \, \frac{36}{43}, \, -\frac{423}{281}, \, \frac{2387}{4511} \right\}.$$

The reader should be careful with making predictions. For instance, the data above suggests that the signs alternate. This is not true: x_{16} and x_{17} are both positive.

The first result about $\{x_n\}$ was established by T. Amdeberhan, L. Medina, and V. Moll in the paper [**12**].

Theorem 12.14.6. *The only time $x_n = 0$ is for $n = 3$.*

The proof of this result is based on a study of the 2-adic valuations described next.

Theorem 12.14.7. *Let $n > 3$ be an integer and let $N = \lfloor \frac{n}{4} \rfloor$. The 2-adic valuation of x_n is given by*

$$\nu_2(x_n) \quad = \quad \begin{cases} \nu_2(2N(N+1)) & \text{if } n \equiv 0,\, 3 \bmod 4, \\ 0 & \text{if } n \equiv 1,\, 2 \bmod 4. \end{cases}$$

In particular, $x_n \neq 0$.

The beginning of the sequence $\{x_n\}$ shows integer entries for $1 \leq n \leq 4$. Given the form of the recurrence, this is not expected. In order to analyze this phenomenon, define the sequence of fractional parts by

$$y_n := \{x_n\} = x_n - \lfloor x_n \rfloor.$$

Figure 12.14.1 shows the sequence $\{x_n\}$ for $1 \leq n \leq 50000$, and Figure 12.14.2 shows the fractional parts y_n and y_{2n}. Observe the presence of *granular* regions combined with some *solid curve* regions. This combination persists as n increases.

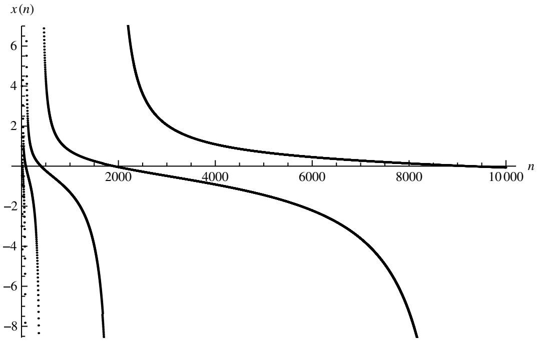


Figure 12.14.1. The sequence x_n.

The sequence $\{y_n\}$ has interesting dynamical properties that the author has been unable to figure out. An example of this is the **lack of intrusion** between the curves and the granular region observed in the figure to the right of Figure 12.14.2.

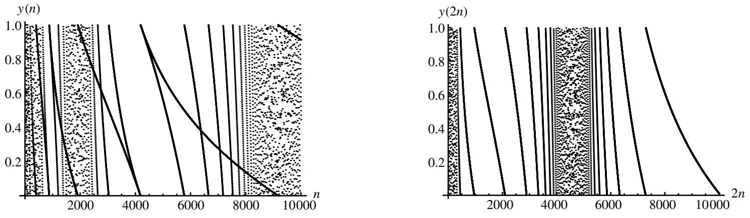


Figure 12.14.2. The fractional parts of x_n and x_{2n}.

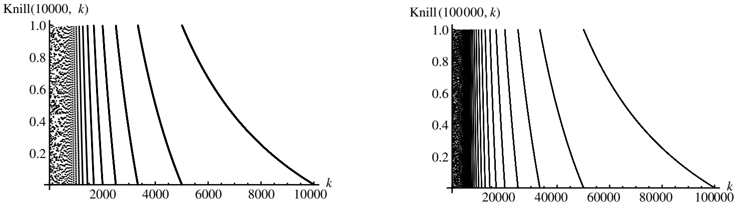


Figure 12.14.3. The dynamics of the Knill map.

Note 12.14.8. O. Knill [**185**] reports on a similar phenomenon for the function

$$f_n(k) = \frac{n \bmod k}{k},$$

for fixed $n \in \mathbb{N}$. The two parts of Figure 12.14.3 show the data for $n = 10000$ and $n = 100000$, respectively. In this case, there is no reappearance of the granular regions.

The next question has eluded the effort of the author:

Conjecture 12.14.9. *The number x_n is not an integer for $n > 4$.*

An interesting sequence of integers f_n appears connected to $\{x_n\}$. The details are given in the next exercise. The author wishes to thank P. Deift for the recurrence for f_n.

Exercise 12.14.10. Check that the recurrence for x_n implies

$$(n+1)x_n - 1 = -2 - \frac{1}{n} + \frac{(n+1)(n+n^{-1})}{1 - nx_{n-1}}.$$

Let $u_n = nx_{n-1} - 1$ and define f_n recursively by $f_1 = 1$ and $f_n = u_n f_{n-1}$. Prove that f_n satisfies the recurrence

$$f_{n+1} = -\frac{2n+1}{n} f_n - \frac{(n+1)(n^2+1)}{n} f_{n-1}.$$

Even though it is not obvious from the recurrence, the numbers f_n are integers. Prove this by establishing the identity

$$f_n = (-1)^{n+1} \operatorname{Re} \prod_{k=0}^{n} (1 + ik).$$

Hint: Look into Sloane's database.

Note 12.14.11. The trigonometric functions are sometimes called **circular functions** as they are defined from the unit circle. These functions are complemented by the **hyperbolic functions** defined in terms of the exponential by

$$\sinh x = \frac{e^x - e^{-x}}{2} \quad \text{and} \quad \cosh x = \frac{e^x + e^{-x}}{2}.$$

As an alternative, these functions can be given a treatment parallel to the one described here for trigonometric functions. The definition is given in terms of the curve

$$\mathcal{H} := \{(u, v) \in \mathbb{R}^2 : u^2 - v^2 = 1\}. \tag{12.14.8}$$

The **hyperbolic angle** $x \in \mathbb{R}$ is defined as the angle of the line joining the origin to the point $(u, v) \in \mathcal{H}$. The hyperbolic functions are defined as

$$\cosh x = u \quad \text{and} \quad \sinh x = v. \tag{12.14.9}$$

The basic relation of Euler

$$e^{ix} = \cos x + i \sin x \tag{12.14.10}$$

gives a relation between hyperbolic and circular functions:

$$\cos ix = \cosh x \quad \text{and} \quad \sin ix = i \sinh x. \tag{12.14.11}$$

It is natural to ask whether there is a third family of functions, now associated to an ellipse. These are the **elliptic functions** and their theory is slightly more complicated. The reader will find information about them in the book by H. McKean and V. Moll [**213**].

Chapter 13

Bernoulli Polynomials

13.1. Introduction

The **Bernoulli polynomials** $B_a(x)$ were introduced in Definition 4.2.4 by the relation

$$B_a(n) = B_a + a\sum_{k=1}^{n-1} k^{a-1}, \tag{13.1.1}$$

valid for $a, n \in \mathbb{N}$ with $a > 1$. Theorem 4.2.1 shows that $B_a(n)$ is a polynomial in n of degree a, with constant term $B_a = B_a(0)$. The value of the constant B_a was defined by the normalization

$$\int_0^1 B_a(x)\,dx = 0. \tag{13.1.2}$$

This chapter contains properties of these polynomials. In particular, an equivalent definition of $B_a(n)$ is provided in Definition 13.2.1.

Example 13.1.1. The evaluation of $B_a(n) - B_a$ may be computed by a finite evaluation. The case $a = 4$,

$$B_4(n) - B_4 = 4\sum_{k=1}^{n-1} k^3, \tag{13.1.3}$$

illustrates the point. The left-hand side is a polynomial of degree 4 in n. Therefore its coefficients may be computed by evaluating the right-hand side at five points. Let $R_4(n)$ denote, temporarily, the right-hand side of (13.1.3) and compute the table of values

(13.1.4)

n	2	3	4	5	6
$R_4(n)$	4	36	144	400	900

.

The Lagrange interpolating polynomial, given in Exercise 4.2.7, shows that $R_4(n) = n^2(n-1)^2$. Therefore, the Bernoulli polynomial of degree 4 is

$$B_4(x) = x^4 - 2x^3 + x^2 - \frac{1}{30}. \tag{13.1.5}$$

The next section gives a second motivation for the choice of the constant B_a.

13.2. The exponential generating function

This section describes a natural choice for B_a in the definition (13.1.1). Consider the sum

$$\begin{aligned} \sum_{a=0}^{\infty} \left[B_a(n) - B_a \right] \frac{t^a}{a!} &= \sum_{a=1}^{\infty} \frac{t^a}{(a-1)!} \sum_{k=1}^{n-1} k^{a-1} \\ &= t \sum_{k=1}^{n-1} \sum_{a=0}^{\infty} \frac{(tk)^a}{a!} \\ &= \frac{te^{nt}}{e^t - 1} - \frac{t}{e^t - 1}. \end{aligned}$$

Comparing the terms independent of n provides a second definition for the Bernoulli number B_a.

Definition 13.2.1. The **Bernoulli numbers** B_a are defined by

$$\frac{t}{e^t - 1} = \sum_{a=0}^{\infty} B_a \frac{t^a}{a!}. \tag{13.2.1}$$

The **Bernoulli polynomials** $B_a(x)$ are defined by

$$\frac{te^{xt}}{e^t - 1} = \sum_{a=0}^{\infty} B_a(x) \frac{t^a}{a!}. \tag{13.2.2}$$

Note 13.2.2. The computation presented above shows that the identity (13.1.1) holds if $B_a(x)$ and B_a are given by Definition 13.2.1.

Exercise 13.2.3. Check the consistency of these definitions. In particular, show that

$$\int_0^1 B_a(x)\,dx = 0 \tag{13.2.3}$$

follows from Definition 13.2.1.

Exercise 13.2.4. Prove that $B_a(0) = B_a$.

Exercise 13.2.5. Use the generating function (13.2.2) to compute

$$\begin{aligned}
B_0(x) &= 1,\\
B_1(x) &= x - \tfrac{1}{2},\\
B_2(x) &= x^2 - x + \tfrac{1}{6},\\
B_3(x) &= x^3 - \tfrac{3}{2}x^2 + \tfrac{1}{2}x,\\
B_4(x) &= x^4 - 2x^3 + x^2 - \tfrac{1}{30}.
\end{aligned}$$

13.3. Elementary properties of Bernoulli numbers

The discussion of Bernoulli numbers begins with a recurrence.

Proposition 13.3.1. *The Bernoulli numbers satisfy*

$$\sum_{k=1}^{a} \binom{a}{k} B_{a-k} = 0, \tag{13.3.1}$$

for $a > 1$.

Proof. The generating function for B_a can be expressed as

$$\begin{aligned}
t &= (e^t - 1) \times \sum_{a=0}^{\infty} B_a \frac{t^a}{a!}\\
&= \sum_{k=1}^{\infty} \frac{t^k}{k!} \times \sum_{a=0}^{\infty} B_a \frac{t^a}{a!}\\
&= \sum_{k,a} \frac{B_a}{k!\,a!} t^{a+k}.
\end{aligned}$$

Now let $r = a + k$ and eliminate the index a to obtain

$$t = \sum_{r=1}^{\infty} \left[\sum_{k=1}^{r} \frac{B_{r-k}}{k!\,(r-k)!} \right] t^r.$$

The result follows by matching equal powers of t. □

Corollary 13.3.2. *The Bernoulli numbers B_a are rational numbers.*

Proof. The identity (13.3.1), for $a > 0$, can be written as

$$B_a = -\frac{1}{a+1} \sum_{j=0}^{a-1} \binom{a+1}{j} B_j. \tag{13.3.2}$$

The result follows by induction on a. □

Exercise 13.3.3. Use the recurrence to confirm the first few values of B_a. The numerators can get very large; for example,

$$B_{38} = \frac{2929993913841559}{6}$$

and

$$B_{40} = -\frac{261082718496449122051}{13530}.$$

Clearly this should not be done by hand.

The data suggests that B_1 is the only nonzero odd Bernoulli number and that the sign of B_{2a} alternates. The first fact is easy to prove.

Proposition 13.3.4. *The value $B_1 = -\frac{1}{2}$ is the only nonzero Bernoulli number with an odd index.*

Proof. The function

$$\frac{t}{e^t - 1} - 1 + \frac{t}{2} = \frac{t}{2} \left[\frac{e^{t/2} + e^{-t/2}}{e^{t/2} - e^{-t/2}} \right] - 1 \tag{13.3.3}$$

is an even function. The result follows from the generating function for B_a. □

Exercise 13.3.5. Make a list of the denominators of the even Bernoulli numbers. This is how it starts:

1, 6, 30, 42, 30, 66, 2730, 6, 510, 798, 330, 138, 2730, 6, 870.

The fact that the denominator of B_a is often 6 will be discussed in Section 13.6. The first values for which this happens are

$$2,\ 14,\ 26,\ 34,\ 38,\ 62,\ 74,\ 86,\ 94,\ 98. \tag{13.3.4}$$

Figure 13.3.1 shows the density of indices with denominator 6.

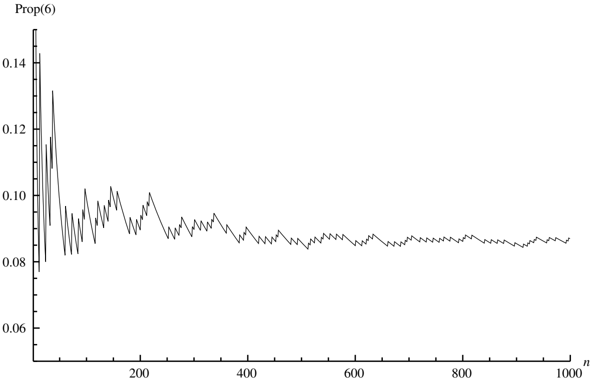


Figure 13.3.1. Proportion of indices with denominator 6.

The next property deals with the structure of the signs of B_a. The proof presented here appears in the paper by L. Mordell [**223**].

Theorem 13.3.6. *For $a > 1$, the Bernoulli numbers satisfy*

$$B_{2a} \quad = \quad -\sum_{r=0}^{a-1} \frac{2^{2r}-1}{2^{2a}-1}\binom{2a}{2r} B_{2r}B_{2a-2r}. \tag{13.3.5}$$

Proof. Write

$$\frac{t}{e^t-1} = \sum_{a=0}^{\infty} B_a \frac{t^a}{a!}$$

so that $B_0 = 1$, $B_1 = -1/2$, and $B_{2a+1} = 0$ for $a > 1$. Then

$$\begin{aligned} \frac{t}{e^t+1} &= \frac{t}{e^t-1} - \frac{2t}{e^{2t}-1} \\ &= -\sum_{a=0}^{\infty}(2^a-1)B_a\frac{t^a}{a!}. \end{aligned}$$

Multiply by $t/(e^t-1)$ so the left-hand side becomes $t^2/(e^{2t}-1)$ and expanding yields

$$\frac{t}{2}\sum_{a=0}^{\infty} B_a 2^a \frac{t^a}{a!} \quad = \quad -\left(\sum_{r=0}^{\infty}(2^r-1)B_r\frac{t^r}{r!}\right)\times\left(\sum_{s=0}^{\infty}B_s\frac{t^s}{s!}\right).$$

Now equate the coefficients of t^{2a} to obtain (13.3.5). □

Corollary 13.3.7. *The even-indexed Bernoulli numbers B_{2a} alternate in sign; that is, they satisfy $(-1)^{a-1}B_{2a}>0$.*

Proof. Define $b_a=(-1)^{a-1}B_{2a}$. Then (13.3.5) becomes

$$b_a=\sum_{r=1}^{a-1}\frac{2^{2r}-1}{2^{2a}-1}\binom{2a}{2r}b_r b_{a-r}. \tag{13.3.6}$$

Therefore $b_a>0$ follows by induction. □

Elementary properties of Bernoulli polynomials. The generating function for the Bernoulli polynomials (13.2.2) is now employed to establish some properties of these polynomials.

Exercise 13.3.8. Prove that for $a\in\mathbb{N}$, the identity

$$B_a(x+1)=B_a(x)+ax^{a-1} \tag{13.3.7}$$

holds.

Note 13.3.9. Identity (13.3.7) and values of $B_a(x)$ for $0\le x\le 1$ determine $B_a(x)$ for all $x\in\mathbb{R}$.

Proposition 13.3.10. *The Bernoulli polynomials $B_a(x)$ satisfy*

$$B_a'(x)=aB_{a-1}(x). \tag{13.3.8}$$

Proof. Differentiate (13.2.2) and use $B_0(x)=1$, to obtain

$$\frac{te^{xt}}{e^t-1}=\sum_{a=1}^{\infty}B_a'(x)\frac{t^{a-1}}{a!}. \tag{13.3.9}$$

Then match powers of t in (13.2.2) to obtain the result. □

Exercise 13.3.11. Prove (13.3.8) by induction on the index a. **Hint:** Use the recurrence (4.2.9) to establish the identity

$$B_{a+1}(x) = B_{a+1} + x^{a+1} - x - \sum_{j=1}^{a-1} \frac{\binom{a+1}{j}}{j+1} \left[B_{j+1}(x) - B_{j+1} \right]$$

and then use (13.3.2).

Exercise 13.3.12. Check that $B_a(1) = B_a(0)$ for $a \geq 2$. Compare these values for $a = 0$ and $a = 1$.

Exercise 13.3.13. Check the special value

$$B_a\left(\tfrac{1}{2}\right) = -(1 - 2^{1-a}) B_a, \quad \text{for } a \geq 2.$$

Exercise 13.3.14. Use the generating function (13.2.2) to prove that

$$B_a(1-x) = (-1)^a B_a(x).$$

This provides symmetry of $B_a(x)$ about the middle point $x = \frac{1}{2}$.

Exercise 13.3.15. The map

$$\mathfrak{D}(P(x)) = P(x+1) - P(x) \tag{13.3.10}$$

acts on the space of polynomials. The identity (13.3.7) shows that the polynomial $g_a(x) = B_a(x)/a$ satisfies

$$\mathfrak{D}(g_a) = x^{a-1}. \tag{13.3.11}$$

Prove that if

$$Q(x) = \sum_{r=0}^{m} q_r x^r,$$

then

$$Q_+(x) = \sum_{r=0}^{m} \frac{q_r}{r+1} B_{r+1}(x)$$

is the **discrete primitive** of Q, that is, $\mathfrak{D}(Q_+(x)) = Q(x)$.

The Bernoulli polynomials can be expressed just using Bernoulli numbers.

Theorem 13.3.16. *The Bernoulli polynomials are given by*

$$B_a(x) = \sum_{j=0}^{a} \binom{a}{j} B_j x^{a-j}.$$

Proof. The generating function gives

$$\begin{aligned}\sum_{a=0}^{\infty} B_a(x)\frac{t^a}{a!} &= \frac{te^{xt}}{e^t-1} = e^{xt} \times \frac{t}{e^t-1} \\ &= \left[\sum_{k=0}^{\infty} \frac{1}{k!}x^k t^k\right] \times \left[\sum_{j=0}^{\infty} \frac{1}{j!}B_j t^j\right] \\ &= \sum_{k,j} \frac{B_j}{j!\,k!} t^{k+j} x^k \\ &= \sum_{a=0}^{\infty} \left[\sum_{j=0}^{a} \binom{a}{j} B_j x^{a-j}\right] \frac{t^a}{a!}.\end{aligned}$$

This gives the stated formula. □

Exercise 13.3.17. The starting point of the evaluation of sums of powers is now written in complete form:

$$\sum_{k=1}^{n-1} k^{a-1} = \frac{1}{a}\sum_{j=0}^{a-1}\binom{a}{j} B_j n^{a-j}, \qquad \text{for } a > 1.$$

Check this identity.

The set of Bernoulli polynomials $\mathbb{B}_n := \{B_a(x) : 0 \leq a \leq n\}$ forms a basis for the vector space of polynomials of degree less than or equal to n. In particular, the polynomial x^j $(0 \leq j \leq n)$ is a linear combination of elements in $\mathbb{B}_n$. The next exercise gives the explicit values of the coefficients.

Exercise 13.3.18. Prove the **inversion formula**

$$x^n = \frac{1}{n+1}\sum_{j=0}^{n}\binom{n+1}{j} B_j(x).$$

Exercise 13.3.19. Prove the **addition theorem**

$$B_a(x+y) = \sum_{j=0}^{a}\binom{a}{j} B_j(x) y^{a-j}.$$

Exercise 13.3.20. Prove the **duplication formula**

$$B_a(2x) = 2^{a-1}\left[B_a(x) + B_a(x+\tfrac{1}{2})\right].$$

This is similar to the trigonometric identity

$$\cot 2x = \cot x + \cot(x + \tfrac{1}{2}).$$

Exercise 13.3.21. Establish the **multiplication formula**

$$B_a(mx) = m^{a-1} \sum_{k=0}^{m-1} B_a\left(x + \frac{k}{m}\right), \quad \text{for } m \in \mathbb{N}.$$

Other sequences of numbers defined in terms of Bernoulli numbers. The expansion of some basic functions is now given in terms of the Bernoulli numbers. The first result requires some elementary complex variables.

Example 13.3.22. The expansion of the cotangent function around $x = 0$ is

$$\cot x = \sum_{n=0}^{\infty} (-1)^n \frac{2^{2n}}{(2n)!} B_{2n} x^{2n-1}. \tag{13.3.12}$$

To establish this expansion, write

$$\cot x = i\left(1 + \frac{2}{e^{2ix} - 1}\right). \tag{13.3.13}$$

Replacing x by $t/2i$ and using the expansion (13.2.1) gives (13.3.12).

Exercise 13.3.23. The tangent numbers T_n are defined in (12.4.6) by the expansion

$$\tan x = \sum_{n=0}^{\infty} T_n \frac{x^n}{n!}. \tag{13.3.14}$$

Use the identity

$$\cot x - 2\cot 2x = \tan x \tag{13.3.15}$$

to produce

$$T_n = \begin{cases} 0 & \text{if } n \text{ is even,} \\ (-1)^{(n-1)/2} 2^{n+1}(2^{n+1} - 1)\frac{B_{n+1}}{n+1} & \text{if } n \text{ is odd.} \end{cases}$$

The fact that the tangent numbers are positive, established in Theorem 12.4.4, gives a new proof of $(-1)^{n-1}B_{2n} > 0$. This appears in the paper by L. Carlitz [**92**].

Note 13.3.24. The previous exercise provides the expansion

$$\tan x = \sum_{n=1}^{\infty} \frac{(-1)^{n-1}2^{2n}}{(2n)!}(2^{2n}-1)B_{2n}x^{2n-1}. \tag{13.3.16}$$

Exercise 13.3.25. Use (13.3.16) to establish

$$\operatorname{cosec} x = \sum_{n=0}^{\infty}(-1)^{n-1}\frac{(2^{2n}-2)}{(2n)!}B_{2n}x^{2n-1}. \tag{13.3.17}$$

This explains why calculus courses discuss the Taylor series of $\sin x$ and $\cos x$, but not the other four trigonometric functions.

Note 13.3.26. The series for **secant** is not in the list of functions whose coefficients depend on Bernoulli numbers. Define the numbers E_n by the expansion

$$\sec x = \sum_{n=0}^{\infty} \frac{E_n}{n!}x^n. \tag{13.3.18}$$

The fact that sec x is an even function shows that $E_n = 0$ for n odd and (13.3.18) is written as

$$\sec x = \sum_{n=0}^{\infty} \frac{E_{2n}}{(2n)!}x^{2n}.$$

The numbers $E_n^* = E_{2n}$ are called the **secant numbers**, or also **Euler numbers**.

Exercise 13.3.27. Derive a recurrence for the Euler numbers. Prove from there that the E_{2n} are positive integers.

Exercise 13.3.28. Derive an identity for Bernoulli numbers from

$$\sin x = \tan x \times \cos x. \tag{13.3.19}$$

What do you get from the corresponding expression for cotangent?

Identities for Bernoulli numbers. The literature contains a large variety of expressions for Bernoulli numbers. Many of them can be obtained directly from the generating function (13.2.1). A classical identity and a couple of recent additions are presented.

Example 13.3.29. The first result is due to L. Euler. It comes from the elementary observation that the generating function

$$b(t) = \frac{t}{e^t - 1} \tag{13.3.20}$$

satisfies the differential equation

$$b^2(t) = (1-t)b(t) - tb'(t). \tag{13.3.21}$$

This produces

$$\sum_{i=2}^{n-2} \binom{n}{i} B_i B_{n-i} = -(n+1)B_n, \tag{13.3.22}$$

for $n \geq 4$.

Example 13.3.30. The second example described here is due to E. Deeba and D. Rodriguez [**109**]. It yields an infinite number of recurrences for the Bernoulli numbers.

Theorem 13.3.31. *Let $a \in \mathbb{N}$. Then*

$$B_a = \frac{1}{n(1-n^a)} \sum_{i=0}^{a-1} B_i n^i \binom{a}{i} \sum_{j=0}^{n-1} j^{a-i}, \quad \textit{for } n \in \mathbb{N} \textit{ and } n \geq 2.$$

Proof. Start with

$$\frac{1-e^{nx}}{1-e^x} = \sum_{j=0}^{n-1} e^{jx} = \sum_{m=0}^{\infty} \left(\sum_{j=0}^{n-1} j^m \right) \frac{x^m}{m!}.$$

Multiply by $x/(1-e^{nx})$ to obtain

$$\begin{aligned}
\frac{x}{1-e^x} &= \frac{1}{n} \frac{nx}{1-e^{nx}} \cdot \frac{1-e^{nx}}{1-e^x} \\
&= \frac{1}{n} \left(\sum_{k=0}^{\infty} B_k \frac{n^k x^k}{k!} \right) \left(\sum_{m=0}^{\infty} \sum_{j=0}^{n-1} j^m \frac{x^m}{m!} \right)
\end{aligned}$$

and multiplying the series yields

$$\begin{aligned}
\frac{x}{1-e^x} &= \frac{1}{n} \sum_{l=0}^{\infty} \left(\sum_{i=0}^{l} \frac{B_i n^i}{i!} \frac{1}{(l-i)!} \sum_{j=0}^{n-1} j^{l-i} \right) x^l \\
&= \frac{1}{n} \sum_{l=0}^{\infty} \frac{1}{l!} \left(\sum_{i=0}^{l} B_i n^i \binom{l}{i} \sum_{j=0}^{n-1} j^{l-i} \right) x^l.
\end{aligned}$$

It follows that

$$B_a = \frac{1}{n} \sum_{i=0}^{a} B_i n^i \binom{a}{i} \sum_{j=0}^{n-1} j^{a-i}.$$

The result follows by solving for B_a. Observe that this term also appears on the right-hand side. □

Example 13.3.32. Recent activity surrounding the Bernoulli numbers is shown in the paper by G. Rzadkowski [**263**]. The main result is

$$B_{a+1} = \frac{(-1)^{a+1}(a+1)}{2^{a+1}-1} \sum_{k=1}^{a+1} \frac{1}{2^k} \sum_{j=0}^{k-1} (-1)^j \binom{k-1}{j} (j+1)^a.$$

Example 13.3.33. The final example presents a relation between the Bernoulli numbers and the harmonic numbers H_n. Introduce the notation $\beta_i = B_i/i$. The **Miki identity** states that

$$\sum_{i=2}^{n-2} \beta_i \beta_{n-i} - \sum_{i=2}^{n-2} \binom{n}{i} \beta_i \beta_{n-i} = 2H_n \beta_n. \tag{13.3.23}$$

This identity appeared first in the paper by H. Miki [**216**] and it has made its place into sophisticated mathematics in the paper by C. Faber and R. Pandharipande [**124**] and into the world of physics in the work of G. V. Dunne [**115**]. Nice proofs can be found in the paper by I. Gessel [**136**] and in the work of I. V. Artamkin [**29**].

Note 13.3.34. D. Zagier [**319**] defined the rational numbers

$$B_n^* := \sum_{r=0}^{n} \binom{n+r}{2r} \frac{B_r}{n+r}, \quad n > 0,$$

and proved that B_{2n+1}^* is periodic, with period 6 and repeating values

$$\{\tfrac{3}{4}, -\tfrac{1}{4}, -\tfrac{1}{4}, \tfrac{1}{4}, \tfrac{1}{4}, -\tfrac{3}{4}\}.$$

13.4. Integrals involving Bernoulli polynomials

This section contains the evaluation of definite integrals involving the Bernoulli polynomials. The first few examples are direct consequences of the identity established in (13.3.8)

$$B'_{a+1}(x) = (a+1)B_a(x), \quad a \geq 1. \tag{13.4.1}$$

Exercise 13.4.1. Use the definition of Bernoulli polynomials from the generating function to prove that for $a \geq 1$

$$\int_0^1 B_a(x)\,dx = 0. \tag{13.4.2}$$

Exercise 13.4.2. Prove that

$$\int_r^{r+1} B_a(x)\,dx = r^a. \tag{13.4.3}$$

Example 13.4.3. Integrals of Bernoulli polynomials can be used to generate some identities for Bernoulli numbers. For example,

$$\begin{aligned}\int_0^1 xB_a(x)\,dx &= \sum_{j=0}^{a}\binom{a}{j}B_j\int_0^1 x^{a-j+1}\,dx \\ &= \sum_{j=0}^{a}\binom{a}{j}\frac{B_j}{a-j+2}.\end{aligned}$$

On the other hand, integration by parts gives

$$\begin{aligned}\int_0^1 xB_a(x)\,dx &= \frac{1}{a+1}\int_0^1 xB'_{a+1}(x)\,dx \\ &= \frac{1}{a+1}\left[xB_{a+1}(x)\Big|_0^1 - \int_0^1 B_{a+1}(x)\,dx\right] \\ &= \frac{B_{a+1}}{a+1}.\end{aligned}$$

It follows that

$$B_{a+1} = (a+1)\sum_{j=0}^{a}\frac{1}{a-j+2}\binom{a}{j}B_j, \qquad \text{for } a > 1. \tag{13.4.4}$$

Products of two Bernoulli polynomials. The set of polynomials

$$\mathbb{B}_n = \{B_0(x), B_1(x), B_2(x), \ldots, B_n(x)\} \tag{13.4.5}$$

forms a basis for the vector space of polynomials of degree at most n. It follows that there exist numbers such that

$$B_p(x)B_q(x) = \sum_{j=0}^{p+q}\alpha_j(p,q)B_j(x). \tag{13.4.6}$$

The goal of this section is to provide an explicit expression for $\alpha_j(p,q)$.

Exercise 13.4.4. Use the identity

$$\frac{uv}{(e^u-1)(e^v-1)}\times\frac{e^{u+v}-1}{u+v}=\frac{uv}{u+v}+\frac{v}{u+v}\frac{u}{e^u-1}+\frac{u}{u+v}\frac{v}{e^v-1},$$

to conclude that

$$\frac{B_k(x)B_j(x)}{k!\,j!}=\text{the coefficient of } u^kv^j \text{ in}$$
$$\left[1+\sum_{n=2}^{\infty}\frac{uv}{n!}\left(\frac{u^{n-1}+v^{n-1}}{u+v}\right)B_n\right]\times\sum_{m=0}^{\infty}B_m(x)\frac{(u+v)^m}{m!}.$$

This is the end of the exercise.

The next step is to evaluate the coefficient of u^kv^j in the expression obtained by expanding the right-hand side of the previous formula:

$$\sum_{m=0}^{\infty}B_m(x)\frac{(u+v)^m}{m!}+\sum_{n=2}^{\infty}\frac{uv}{n!}\times\frac{u^{n-1}+v^{n-1}}{u+v}B_n$$
$$+\sum_{n=2}^{\infty}\sum_{m=1}^{\infty}\frac{uv}{n!m!}\times(u^{n-1}+v^{n-1})(u+v)^{m-1}B_nB_m(x).$$

The first term is

$$\sum_{m=0}^{\infty}\frac{B_m(x)}{m!}\sum_{t=0}^{m}\binom{m}{t}u^tv^{m-t},$$

and the power u^kv^j yields

$$\text{the first term contribution is } \frac{1}{k!j!}B_{k+j}(x).$$

The second term is

$$\begin{aligned}\sum_{n=2}^{\infty}\frac{uv}{n!}\frac{u^{n-1}+v^{n-1}}{u+v}B_n &= \sum_{n=2}^{\infty}\frac{uv}{n!}B_n\sum_{t=0}^{n-2}(-1)^tu^tv^{n-2-t}\\ &= \sum_{n=2}^{\infty}\frac{1}{n!}B_n\sum_{t=0}^{n-2}(-1)^tu^{t+1}v^{n-1-t}.\end{aligned}$$

To count those that contribute to $u^k v^j$, observe that $k+j=n$. The power of u must be k; therefore $t=k-1$. This gives

$$\text{the second term contribution is } \frac{(-1)^{k-1}}{(k+j)!}B_{k+j}.$$

Exercise 13.4.5. Check that the third term is

$$\sum_{r=1}^{\lfloor (k+j-1)/2 \rfloor} \left[j\binom{k}{2r} + k\binom{j}{2r} \right] \frac{B_{2r}}{k+j-2r} B_{k+j-2r}(x).$$

The discussion above is recorded as the next theorem.

Theorem 13.4.6. *The product of two Bernoulli polynomials is given by*

$$\begin{aligned} B_k(x)B_j(x) = {} & \frac{(-1)^{k-1}k!j!}{s!}B_s \\ & + \sum_{r=0}^{\lfloor (s-1)/2 \rfloor} \left[j\binom{k}{2r} + k\binom{j}{2r} \right] \frac{B_{2r}}{s-2r} B_{s-2r}(x), \end{aligned}$$

with $s=k+j$.

Corollary 13.4.7. *Let k, $j \geq 1$. Then*

$$\int_0^1 B_k(x)B_j(x)\,dx = (-1)^{k-1}\binom{s}{k}^{-1} B_s, \tag{13.4.7}$$

with $s=k+j$.

Exercise 13.4.8. Determine the value of the integral of a product of three Bernoulli polynomials.

13.5. A relation to Stirling numbers

This section discusses a classical identity relation of Bernoulli to Stirling numbers. The proof presented here is completely elementary and it appeared in the paper by G. Rzadkowski [**262**].

Exercise 7.2.3 shows the existence of a family of coefficients $a(n,k)$ such that

$$f^{(n)}(x) = \sum_{k=1}^{n+1} \frac{a(n,k)}{(1+e^x)^k} \tag{13.5.1}$$

for $f(x) = 1/(1+e^x)$. The coefficients $a(n,k)$ are given by

$$a(n,k) = (-1)^{n+k}(k-1)!S(n,k). \tag{13.5.2}$$

Now let $t = 1/(1+e^x)$. Then there is a family of polynomials $A_n(t)$ such that $f^{(n)}(x) = A_{n+1}(t)$.

The proof of the next result follows directly from the definition of $A_{n+1}(t)$.

Lemma 13.5.1. *Let $f(x) = 1/(1+e^x)$ and $g(z,x) := f(z+x)$. The Taylor expansion of g in the variable z is*

$$g(z,x) = \sum_{n=0}^{\infty} A_{n+1}(t)\frac{z^n}{n!} \tag{13.5.3}$$

where $t = 1/(1+e^x)$.

Now observe that

$$g(z,x) = \frac{1}{1+e^{z+x}} = \frac{1}{1+e^z \cdot e^x} = \frac{t}{t+(1-t)e^z}. \tag{13.5.4}$$

Integrating the relation

$$\frac{t}{t+(1-t)e^z} = \sum_{n=0}^{\infty} A_{n+1}(t)\frac{z^n}{n!} \tag{13.5.5}$$

yields

$$\frac{1-e^z+ze^z}{(1-e^z)^2} = \sum_{n=0}^{\infty} \int_0^1 A_{n+1}(t)dt\,\frac{z^n}{n!}. \tag{13.5.6}$$

Exercise 13.5.2. Use the generating function of the Bernoulli polynomials (13.2.2) to prove

$$\int_0^1 A_n(t)\,dt = -B_n. \tag{13.5.7}$$

The relation between the Bernoulli and Stirling numbers is a restatement of (13.5.7).

Proposition 13.5.3. *The Bernoulli numbers satisfy*

$$B_n = -\sum_{k=1}^{n} \frac{a(n-1,k)}{k+1} = \sum_{k=1}^{n} \frac{(-1)^{n+k+1}(k-1)!}{k+1}S(n-1,k).$$

13.6. Arithmetic properties of Bernoulli numbers

The Bernoulli numbers B_{2n} are rational numbers with sign $(-1)^{n-1}$. Let

$$(-1)^{n-1}B_{2n} = \frac{N_{2n}}{D_{2n}} \tag{13.6.1}$$

be the representation with $\gcd(N_{2n}, D_{2n}) = 1$. This section will consider arithmetic properties of N_{2n} and D_{2n}.

The next subsection presents a congruence that is employed later to establish the von Staudt-Clausen theorem, which yields an exact expression for D_{2n}, the denominator of the Bernoulli number B_{2n}. The numerators are discussed next, with particular emphasis on their relation to Fermat's last theorem.

A congruence for the sum of powers. The first result deals with a congruence for the sum $S_a(n)$ defined in (4.2.5) as

$$S_a(n) = \sum_{k=1}^{n-1} k^a, \quad a \in \mathbb{N}_0,\, n > 1. \tag{13.6.2}$$

The proof employs the relation

$$n^{a+1} - 1 = \sum_{j=0}^{a} \binom{a+1}{j} S_j(n) \quad \text{for } n \geq 1,\, a \geq 0 \tag{13.6.3}$$

originally due to B. Pascal [**242**]. This is of intrinsic interest and it has already appeared in Theorem 4.2.1. The argument presented here is due to K. MacMillan and J. Sondow [**207**]. The reader should look back at (4.2.8) before reading the next result.

Proposition 13.6.1. *Let p be a prime. For $a \geq 1$, the congruence*

$$S_a(p) \equiv \begin{cases} -1 \bmod p & \textit{if } p-1 \textit{ divides } a, \\ 0 \quad \bmod p & \textit{if } p-1 \textit{ does not divide } a \end{cases}$$

holds.

The argument is divided into two cases.

Case 1. Assume first that $p-1$ divides a. Then $a=(p-1)t$, with $t\in\mathbb{N}$. Then, Fermat's little theorem (see Subsection 2.5.2) gives

$$S_a(p)\equiv\sum_{k=1}^{p-1}(k^{p-1})^t\equiv\sum_{k=1}^{p-1}1^t=p-1\equiv-1 \bmod p$$

as claimed.

Case 2. If $p-1$ does not divide a, assume that p does not divide $S_a(p)$. Take a to be the smallest positive integer with these properties, namely $a\not\equiv 0 \bmod p-1$ and $S_a(p)\not\equiv 0 \bmod p$. Dividing yields

$$a=(p-1)d+r \quad \text{with } d\geq 0 \text{ and } 0<r<p-1.$$

Then $S_a(p)\equiv S_r(p) \bmod p$. Indeed,

$$S_a(p)=\sum_{k=1}^{p-1}k^a=\sum_{k=1}^{p-1}(k^{p-1})^d\cdot k^r\equiv\sum_{k=1}^{p-1}k^r=S_r(p) \bmod p.$$

Therefore, the value a is in the range $0<a<p-1$. It follows that

$$S_0(p)=p,\quad S_1(p),\,S_2(p),\ldots,S_{a-1}(p)\equiv 0 \bmod p. \tag{13.6.4}$$

Now choose $n=p+1$ in (13.6.3) to obtain

$$(p+1)^{a+1}-1\equiv\sum_{j=0}^{a}\binom{a+1}{j}S_j(p+1) \bmod p. \tag{13.6.5}$$

Now employ the previous congruences and $S_j(p)\equiv S_j(p+1) \bmod p$ to conclude that

$$(a+1)S_a(p)\equiv 0 \bmod p. \tag{13.6.6}$$

The range of values of a shows that p does not divide $a+1$. Thus $S_a(p)\equiv 0 \bmod p$. This is a contradiction.

The von Staudt-Clausen theorem. The next result determines those primes dividing the denominator D_{2n}.

Theorem 13.6.2. *If $n\geq 1$, then the denominator D_{2n} is the product of all primes p such that $p-1$ divides $2n$. In particular 6 divides D_{2n}.*

Proof. The proof is based on considering the terms in the sums appearing in Proposition 13.5.3 that are not integers.

Case 1. If $k+1$ is composite and $k \geq 6$, then $k+1 = a \cdot b$ with a, b relatively prime and appearing in $(k-1)!$ and it follows that $k+1$ divides $(k-1)!$. Therefore this term does not contribute to the denominator of B_n.

Case 2. If $k = 3$, the coefficient of $\frac{1}{4}$ is $2S(n-1,3) = 3^{n-1} - 2^n + 1$ as in Exercise 7.3.3. For n even, this term is divisible by 4, so $k = 3$ does not contribute to the denominator of B_n.

Case 3. If $k+1 = p$ is an odd prime, then the coefficient of $1/p$ is

$$a(n-1,p-1) = \pm(p-2)!S(n-1,p-1) = \pm\sum_{j=0}^{p-2}(-1)^j\binom{p-2}{j}(j+1)^{n-1}.$$

The analysis of this identity employs an auxiliary function.

Lemma 13.6.3. *Let $g_j(x) = e^x(1-e^x)^j$. Then*

$$g_j^{(r)}(0) = \begin{cases} 0 & \textit{if } 0 \leq r < j, \\ (-1)^j\, j! & \textit{if } r = j. \end{cases}$$

Proof. The first derivative is

$$g'(x) = e^x(1-e^x)^j - je^{2x}(1-e^x)^{j-1}.$$

This vanishes if $j > 1$. In order to obtain a nonvanishing value, the exponent in the term $1 - e^x$ has to drop down to zero. This takes j steps.

The analysis of Case 3 is subdivided into two parts:

Case 3a. If $p-1$ divides n, say $n = (p-1)t$, Fermat's little theorem gives

$$j^{n-1} = j^{(p-1)(t-1)+p-2} \equiv j^{p-2} \bmod p \tag{13.6.7}$$

and the coefficient of $1/p$ becomes

$$J := \sum_{j=0}^{p-2}(-1)^j\binom{p-2}{j}(j+1)^{p-2}. \tag{13.6.8}$$

Lemma 13.6.3 states that $J \equiv g^{(p-2)}(0)$. Wilson's theorem shows that $J \equiv -1 \bmod p$. It follows that this term contributes to the denominator.

Case 3b. If $p-1$ does not divide n, then $(j+1)^{n-1} \equiv (j+1)^m \bmod p$ for some m in the range $0 \leq m \leq p-3$. Then the coefficient of $1/p$ is $g^{(m)}(0) = 0$ and in this case, k does not contribute to the denominator.

The only missing value is $k = 1$ and it is seen that this term contributes to the denominator. The proof is complete. □

Corollary 13.6.4. *For $n \in \mathbb{N}$ and any prime p, the product pB_{2n} is p-integral, that is, pB_{2n} is a rational number such that p does not divide its denominator. Moreover,*

$$pB_{2n} \equiv \begin{cases} -1 \bmod p & \text{if } p-1 \text{ divides } 2n, \\ 0 \bmod p & \text{otherwise.} \end{cases}$$

Note 13.6.5. The structure of the denominator D_{2n} has now been established. The curious result appears in B. C. Kellner [**183**]:

Theorem 13.6.6. *Let $n \in \mathbb{N}$. Then $D_{2n} = 2n$ if and only if $n = 903$.*

Note 13.6.7. P. Erdős and S. Wagstaff [**119**] have shown that the fractional parts $\{B_{2n}\}$ are dense in the interval $(0,1)$.

Exercise 13.6.8. Let q be a prime of the form $3n+1$. Prove that the denominator of B_{2q} is 6. Make a list of the first twenty primes q that satisfy the hypothesis. **Note:** Dirichlet proved that there are infinitely many primes of the form $3n+1$.

Note 13.6.9. T. S. Caley in his master thesis [**87**] reviews a large variety of proofs of the von Staudt-Clausen theorem. There are many interesting results quoted in this thesis. The author wishes to thank K. Dilcher for pointing out this work. The following result, due to R. J. McIntosh [**211**], is particularly beautiful. It relates the Fermat numbers $f_n = 2^{2^n}+1$ defined in Note 1.7.10 and the tangent numbers T_n defined in (12.4.6).

Theorem 13.6.10. *The Fermat number f_n is prime if and only if f_n does not divide the tangent number T_{f_n-2}.*

The numerators of Bernoulli numbers. These numbers are much harder to characterize than the denominators and the intrinsic interest in their factorization comes from the next theorem of Kummer.

Definition 13.6.11. A prime p is called **regular** if p does not divide the numerators of the Bernoulli numbers B_{2n} with $2 \leq 2n \leq p-3$.

Theorem 13.6.12. *The equation* $x^p + y^p = z^p$ *has no solution with* $xyz \neq 0$ *if* p *is a regular prime.*

One of the earliest results on the factorization of N_{2n} is the next theorem due to J. C. Adams [**1**].

Theorem 13.6.13. *Let* $n \in \mathbb{N}$ *and let* p *be a prime such that* $p-1$ *does not divide* $2n$*. If* p^e *divides* $2n$*, then* p^e *divides* N_{2n}*.*

For example, 5^2 divides N_{50}. Indeed,

$$\begin{aligned} N_{50} &= 495057205241079648212477525 \\ &= 5^2 \cdot 417202699 \cdot 47464429777438199 \end{aligned}$$

and the prime factorization of N_{98} is

$$\begin{aligned} N_{98} = 7^2 \cdot 2857 \cdot 3221 \cdot 1671211 \cdot 9215789693276607167 \\ \cdot 977826315287499621858461730718054961643559 9. \end{aligned}$$

These two examples indicate the difficulties in providing a simple criterion for deciding when a prime divides the numerator N_{2n}. On the other hand, there is a certain peridiocity related to this divisibility. This is expressed by the **Kummer congruences** given in the next theorem.

Theorem 13.6.14. *If* $n \geq 1$ *and* $p \geq 5$ *is a prime such that* $p-1$ *does not divide* $2n$*, then*

$$\frac{B_{2n+(p-1)}}{2n+(p-1)} \equiv \frac{B_{2n}}{2n} \bmod p.$$

In particular, if p *divides some numerator* N_{2n}*, then it divides every* $(p-1)$*st numerator after that.*

13.7. The Euler-MacLaurin summation formula

This is a procedure that is employed to compare the integral of a function with the sum of its values at the integers, that is, the quantities

$$\int_1^n f(x)\,dx \quad \text{and} \quad \sum_{i=1}^n f(i).$$

The simplest instance of such a comparison occurs when the function $f(x)$ is assumed to be decreasing and with finite integral on $[1,\infty)$. Then the inequality

$$\sum_{i=2}^n f(i) \leq \int_1^n f(x)\,dx \leq \sum_{i=1}^{n-1} f(i)$$

can be established by integrating the bounds $f(i) \leq f(x) \leq f(i-1)$ on the interval $[i-1,i]$ and then summing over i. Introduce the notation

$$b_n(f) = \sum_{i=1}^n f(i) - \int_1^n f(x)\,dx.$$

The previous argument shows that if f is nonnegative and decreasing, then

$$f(n) \leq b_n(f) \leq f(1),$$

that is, $b_n(f)$ is a bounded sequence. The question considered here is how to proceed when the function is not necessarily monotone and to provide estimates for the **error term** $b_n(f)$. The material presented here is classical. One of the best presentations is given in the paper by T. Apostol [**27**].

The comparison between sums and integrals is now extended to a general class of functions. Start with the identity

$$\int_1^n f(x)\,dx = \sum_{k=1}^n \int_k^{k+1} f(x)\,dx,$$

which may be written in the form

$$\int_1^n f(x)\,dx + f(1) - \sum_{k=1}^n f(k) = \sum_{k=1}^{n-1} \int_k^{k+1} \left[f(x) - f(k+1) \right]\,dx,$$

to have the integrand vanish at the upper limit of integration. Denote the integral on the right-hand side by J_k. Now integrate by parts using $x + C_k$ as the primitive of the factor 1, with a constant C_k to be determined. This gives

$$\begin{aligned} J_k &= \int_k^{k+1} [f(x) - f(k+1)] \cdot 1 \, dx \\ &= -(k + C_k)[f(k) - f(k+1)] - \int_k^{k+1} (x + C_k) f'(x) \, dx. \end{aligned}$$

The choice $C_k = -k - 1$ gives

$$J_k = f(k) - f(k+1) - \int_k^{k+1} (x - k - 1) f'(x) \, dx.$$

The identity $\lfloor x \rfloor = k$ holds in the interval of integration. Therefore

$$J_k = f(k) - f(k+1) - \int_k^{k+1} (x - \lfloor x \rfloor - 1) f'(x) \, dx.$$

This produces

$$\int_1^n f(x) \, dx + f(1) = \sum_{k=1}^n f(k) + \int_1^n (x - \lfloor x \rfloor) f'(x) \, dx.$$

Exercise 13.7.1. Show that the previous identity may be written in the form

$$\int_1^n f(x) \, dx = \sum_{k=1}^n f(k) + \int_1^n f'(x) P_1(x) \, dx + \frac{1}{2}(f(n) + f(1)),$$

with

$$P_1(x) = \begin{cases} x - \lfloor x \rfloor - \frac{1}{2} & \text{if } x \notin \mathbb{Z}, \\ 0 & \text{if } x \in \mathbb{Z}. \end{cases}$$

Prove that the function $P_1(x)$ is periodic and its integral over $[0, 1]$ is zero. The reader will recognize $P_1(x)$ as the **periodic extension** of the Bernoulli polynomial $B_1(x) = x - 1/2$.

Exercise 13.7.2. Assume the functions f and f' are continuous with

$$\lim_{n \to \infty} f(n) = 0 \quad \text{and} \quad \lim_{n \to \infty} \int_n^\infty |f'(x)| \, dx = 0.$$

Establish the identity

$$\sum_{k=1}^n f(k) = \int_1^n f(x) \, dx + C(f) + E_f(n)$$

with

$$C(f) = \frac{f(1)}{2} + \int_1^\infty P_1(x) f'(x)\,dx$$

and

$$E_f(n) = \frac{f(n)}{2} - \int_n^\infty P_1(x) f'(x)\,dx.$$

Under these conditions $\lim_{n\to\infty} E_f(n) = 0$ and

$$\lim_{n\to\infty}\left[\sum_{k=1}^n f(k) - \int_1^n f(x)\,dx\right] = C(f).$$

This section concludes with an extension of Exercise 13.7.1. The proof follows the arguments presented here. The details may be found in [**27**].

Theorem 13.7.3 (General form of Euler's summation formula). *For any function f with a continuous derivative of order $2m+1$ on the interval $[1, n]$, the formula*

$$\begin{aligned}\sum_{k=1}^n f(k) \quad &= \quad \int_1^n f(x)\,dx + \frac{1}{(2m+1)!}\int_1^n P_{2m+1}(x) f^{(2m+1)}(x)\,dx \\ &\quad + \sum_{r=1}^m \frac{B_{2r}}{(2r)!}\left(f^{(2r-1)}(n) - f^{(2r-1)}(1)\right) + \frac{f(1)+f(n)}{2}\end{aligned}$$

holds. The function $P_j(x)$ is the periodic extension of the Bernoulli polynomial, defined by

$$P_j(x) = B_j(x - \lfloor x \rfloor).$$

Moreover, if the improper integral $\int_1^\infty |f^{(2m+1)}(x)|\,dx$ converges, then

$$\sum_{k=1}^n f(k) = \int_1^n f(x)\,dx + C(f) + E_f(n),$$

where

$$\begin{aligned}C(f) \quad &= \quad \frac{f(1)}{2} - \sum_{r=1}^m \frac{B_{2r}}{(2r)!} f^{(2r-1)}(1) \\ &\quad + \frac{1}{(2m+1)!}\int_1^\infty P_{2m+1}(x) f^{(2m+1)}(x)\,dx\end{aligned}$$

and

$$\begin{aligned} E_f(n) &= \frac{f(n)}{2} + \sum_{r=1}^{m} \frac{B_{2r}}{(2r)!} f^{(2r-1)}(n) \\ &\quad - \frac{1}{(2m+1)!} \int_n^\infty P_{2m+1}(x) f^{(2m+1)}(x)\,dx. \end{aligned}$$

Exercise 13.7.4. Convince yourself that $C(f)$ is **independent** of m.

Example 13.7.5. Let $f(x) = 1/x$. First take $m = 0$ in Theorem 13.7.3 to obtain

$$\sum_{k=1}^{n} \frac{1}{k} = \int_1^n \frac{dx}{x} - \int_1^n \frac{P_1(x)}{x^2}\,dx + \frac{1+1/n}{2}.$$

This can be written as

$$H_n = \ln n - \int_1^n \frac{\{x\} - \frac{1}{2}}{x^2}\,dx + \frac{1}{2} + \frac{1}{2n}, \tag{13.7.1}$$

where the H_n are the harmonic numbers defined in (11.11.1). The bound $|\{x\} - \frac{1}{2}| \le \frac{3}{2}$ shows that the integral in (13.7.1) converges as $n \to \infty$. It follows that

$$H_n - \ln n = \frac{1}{2} - \int_1^\infty \frac{\{x\} - \frac{1}{2}}{x^2}\,dx + \int_n^\infty \frac{\{x\} - \frac{1}{2}}{x^2}\,dx + \frac{1}{2n}. \tag{13.7.2}$$

The terms on the right-hand side that depend on n constitute the error term

$$E_f(n) = \int_n^\infty \frac{\{x\} - \frac{1}{2}}{x^2}\,dx + \frac{1}{2n}, \tag{13.7.3}$$

and the limiting value on the right-hand side (as $n \to \infty$) is

$$C(f) = \frac{1}{2} - \int_1^\infty \frac{\{x\} - \frac{1}{2}}{x^2}\,dx. \tag{13.7.4}$$

Then (13.7.2) is

$$H_n - \ln n = C(f) + E_f(n). \tag{13.7.5}$$

Definition 13.7.6. The limit

$$\gamma = \lim_{n \to \infty} H_n - \ln n \tag{13.7.6}$$

exists and is called the **Euler**, or **Euler-Mascheroni**, constant.

The previous discussion provides the integral representation

$$\gamma = \frac{1}{2} - \int_1^\infty \frac{\{x\} - \frac{1}{2}}{x^2}\, dx. \tag{13.7.7}$$

Exercise 13.7.7. Prove the bound $|E_f(n)| \leq \frac{2}{n}$.

Example 13.7.8. Let $f(x) = 1/x$ as in the previous example, but this time take $m = 1$ in Theorem 13.7.3. This gives

$$\sum_{k=1}^{n} \frac{1}{k} = \int_1^n \frac{dx}{x} + \frac{1}{6} \int_1^n P_3(x) \times \left(\frac{-6}{x^4} \right) dx + \frac{1}{12}\left(-\frac{1}{n^2} + 1 \right) + \frac{1}{2}\left(1 + \frac{1}{n} \right).$$

This may be written as

$$H_n = \ln n - \int_1^n \frac{P_3(x)}{x^4}\, dx + \frac{7}{12} + \frac{1}{2n} - \frac{1}{12n^2}. \tag{13.7.8}$$

Exercise 13.7.9. Compute $P_3(x)$ and check that $|P_3(x)| \leq 3$.

Thus, the integral in (13.7.8) converges as $n \to \infty$ and it follows that

$$H_n - \ln n = C(f) + E_f(n) \tag{13.7.9}$$

with

$$C(f) = -\int_1^\infty \frac{P_3(x)}{x^4}\, dx + \frac{7}{12} \tag{13.7.10}$$

and

$$E_f(n) = \int_n^\infty \frac{P_3(x)}{x^4}\, dx + \frac{1}{2n} - \frac{1}{12n^2}. \tag{13.7.11}$$

Exercise 13.7.10. Check the second integral representation for Euler constant

$$\gamma = \frac{7}{12} - \frac{1}{2} \int_1^\infty \frac{\{x\} - 3\{x\}^2 + 2\{x\}^3}{x^4}\, dx.$$

Estimate the error $E_f(n)$ in (13.7.11). **Hint:** The numerator of the integrand is bounded by $1/6\sqrt{3} < 1/10$.

Exercise 13.7.11. Give the details for $m = 2$.

Note 13.7.12. The form of the error term obtained in the two previous examples suggests the existence of a sequence of numbers e_j such that

$$E_f(n) = \frac{e_1}{n} + \frac{e_2}{n^2} + \frac{e_3}{n^3} + \cdots + \frac{e_r}{n^r} + \int_n^\infty h_r(x)\,dx,$$

where the number of terms r and the function $h_r(x)$ depend upon the choice of m. The question is, *why not just let $m \to \infty$ and obtain a series approximation of the error term*? It turns out that such a procedure diverges and the expression for the error term makes sense only for **finite and fixed** m. This is the subject of **asymptotic expansions**. The reader will find a nice introduction to this topic in N. M. Temme [**289**].

Example 13.7.13. The next example gives an asymptotic expansion for factorials that will include Stirling's formula. This states that

$$\lim_{n\to\infty} \frac{n!}{e^{-n}n^{n+1/2}} = \sqrt{2\pi}. \tag{13.7.12}$$

The existence of the limit was established in Theorem 2.10.1 and its value was obtained in Exercise 12.6.4 as a consequence of Wallis' infinite product for π given in (12.6.3).

Take $f(x) = \ln x$ and $m = 0$ in Theorem 13.7.3 to obtain

$$\sum_{k=1}^n \ln k = \int_1^n \ln x\,dx + \int_1^n \frac{P_1(x)}{x}\,dx + \frac{\ln n}{2},$$

with $P_1(x) = \{x\} - \frac{1}{2}$. This is written as

$$\ln n! = 1 - n + n\ln n + \frac{\ln n}{2} + \int_1^n \frac{P_1(x)}{x}\,dx. \tag{13.7.13}$$

The analysis of the behavior of the last integral as $n \to \infty$ is not so elementary. It is not possible to simply bound $P_1(x)$ because the function $1/x$ has a divergent integral. The result follows from the next theorem.

Theorem 13.7.14 (Dirichlet's test for improper integrals). *Assume f and g are continuous functions with f monotonically decreasing on $[a,\infty)$ and with $f(x) \to 0$ as $x \to \infty$. Moreover, assume there is a constant M such that*

$$\left|\int_a^x g(t)\,dt\right| \leq M$$

for all $x \geq a$. Then

$$\int_a^\infty f(x)g(x)\,dx < \infty.$$

The reader will find a proof in the book by K. R. Stromberg [**285**].

Exercise 13.7.15. Check carefully that Dirichlet's theorem may be used to conclude the convergence of the integral of $P_1(x)/x$. **Hint:** Approximate P_1 by a continuous function.

The identity (13.7.13) is now written as

$$\ln\left[\frac{n!}{e^{-n}n^{n+1/2}}\right] = \left(1 + \int_1^\infty \frac{P_1(x)}{x}\,dx\right) - \int_n^\infty \frac{P_1(x)}{x}\,dx.$$

It follows from this that the limit (13.7.12) exists, and from its value the integral evaluation

$$\int_1^\infty \frac{\{x\} - \frac{1}{2}}{x}\,dx = \ln\sqrt{2\pi} - 1 \tag{13.7.14}$$

is obtained. Compare this with the evaluation

$$\int_1^\infty \frac{\{x\} - \frac{1}{2}}{x^2}\,dx = \frac{1}{2} - \gamma \tag{13.7.15}$$

given in (13.7.7).

Exercise 13.7.16. Derive from Theorem 13.7.3 the identity

$$\ln\left[\frac{n!}{e^{-n}n^{n+1/2}}\right] = \frac{11}{12} - \frac{1}{2}\int_1^n \frac{\{x\} - 3\{x\}^2 + 2\{x\}^3}{x^4}\,dx + \frac{1}{12n}.$$

Conclude that

$$\ln\left[\frac{n!}{e^{-n}n^{n+1/2}}\right] = \ln\sqrt{2\pi} + \frac{1}{12n} + \frac{1}{2}\int_n^\infty \frac{\{x\} - 3\{x\}^2 + 2\{x\}^3}{x^4}\,dx.$$

Note 13.7.17. Iterating the process described above gives the expansion

$$\ln\left[\frac{n!}{(n/e)^n\sqrt{2\pi n}}\right] = \frac{1}{12n} - \frac{1}{360n^3} + \frac{1}{1260n^5} - \frac{1}{1680n^7} + \cdots,$$

and exponentiating yields

$$n! \sim n^n e^{-n}\sqrt{2\pi n}\sum_{k\geq 0}\frac{a_k}{n^k}. \tag{13.7.16}$$

The coefficients a_k are usually called the **Stirling coefficients**. The numbers $b_{2k+1} := a_k/(2k+1)!!$ can be computed recursively from

$$b_k = \frac{1}{k+1}\left(b_{k-1} - \sum_{j=2}^{k-1} j b_j b_{k-j+1} \right),$$

starting with $b_0 = b_1 = 1$. G. Nemes [**232**] has provided the exact formula

$$\begin{aligned} a_k = \frac{(2k)!}{2^k k!} \sum_{i=0}^{2k} & \binom{k+i-1/2}{i}\binom{3k+1/2}{2k-i} \\ & \times 2^i \sum_{j=0}^{i} \binom{i}{j} \frac{(-1)^j}{(2k+i+j)!} \sum_{\ell=0}^{j} (-1)^{\ell} \binom{j}{\ell} (j-\ell)^{2k+i+j}. \end{aligned}$$

13.8. Bernoulli numbers and solitons

It is a remarkable fact that the Bernoulli numbers continue to appear in many areas of mathematics. The theory of solitons has not escaped them. The relation begins with the **Korteweg-de Vries** (KdV) equation

$$u_t - 6uu_x + u_{xxx} = 0, \tag{13.8.1}$$

which originally appeared in the context of shallow water waves. It turns out that the KdV equation has an infinite number of conserved quantities of the form

$$I_n[u] = \int P_n(u, u_x, u_{xx}, \ldots, u_n)\, dx \tag{13.8.2}$$

where P_n is a polynomial of u and its x-derivatives up to order n.

One of the many features that makes the KdV equation a special equation is the existence of **solitons**. The simplest example is given by

$$u(x,t) = -2\,\mathrm{sech}^2(x-4t).$$

The reader can easily check that this is a solution of the KdV equation. Recently D. B. Fairlie and A. P. Veselov [**125**] and M. P. Grosset and

A. P. Veselov [**154**] have shown that the conserved quantities of the soliton may be expressed in the form

$$I_{n-1}[-2\lambda \text{sech}^2 x] = (-1)^{n-1} \frac{2^{2n+2}}{2n+1} F_n(\lambda), \tag{13.8.3}$$

where $F_n(\lambda)$ is the **Faulhaber polynomial**, defined in terms of the Bernoulli polynomial by

$$B_{2n+2}(x+1) = (2n+2) F_n \left(\frac{x^2+x}{2} \right) + B_{2n+2}. \tag{13.8.4}$$

From this context, the authors of [**154**] established the identity

$$B_{2n} = \frac{(-1)^{n-1}}{2^{2n+1}} \int_{-\infty}^{\infty} \left[\left(\frac{d}{dx} \right)^{n-1} \text{sech}^2 x \right]^2 dx.$$

This must have been known to Euler, but the present author has not tried to find it in the literature.

13.9. The Giuga-Agoh conjectured criterion for primality

The remainder of the sum

$$G_n := \sum_{k=1}^{n-1} k^{n-1} \tag{13.9.1}$$

modulo n is easy to determine if n is a prime number. Indeed, Fermat's little theorem states that $k^{n-1} \equiv 1 \bmod n$ and it follows that

$$G_n \equiv -1 \bmod n. \tag{13.9.2}$$

G. Giuga [**137**] conjectured that the converse is valid.

Conjecture 13.9.1. *Suppose $G_n \equiv -1 \bmod n$. Then n is prime.*

Note 13.9.2. The notation

$$S_a(n) = \sum_{k=1}^{n-1} k^a \tag{13.9.3}$$

was employed in Chapter 4, so that $G_n = S_{n-1}(n)$ is the reason why the notation employed in the papers by D. H. Bailey and J. M. Borwein [**35**] and D. Borwein, J. M. Borwein, and R. Girgensohn [**68**] is not adopted here. The reader should be careful when reading these papers.

A similar conjectured criterion for primality was developed by T. Agoh [**2**].

Conjecture 13.9.3. *Let B_n be the Bernoulli number. Then*

$$nB_{n-1} \equiv -1 \bmod n \quad \textit{if and only if } n \textit{ is prime.}$$

These conjectures are actually equivalent; see the paper by B. C. Kellner [**184**] for a detailed proof.

D. Borwein et al. [**68**] described properties of possible counterexamples n to the Giuga-Agoh conjecture. In particular, any such composite number must be a **Carmichael number**; that is, $a^{n-1} \equiv 1 \bmod n$ for every choice of a that is relatively prime to n. There are infinitely many Carmichael numbers, as established in the paper by W. R. Alford, A. Granville, and C. Pomerance [**5**]. In [**68**] the authors introduced the concept of a **Giuga number** as a composite number n such that p divides $n/p - 1$, for all prime divisors of n. Any Giuga number is square-free. It is possible to describe Giuga numbers in a style similar to Conjecture 13.9.3.

Theorem 13.9.4. *The number n is a Giuga number if and only if*

$$nB_{\varphi(n)} \equiv -1 \bmod n.$$

The next beautiful characterization was provided by Giuga.

Theorem 13.9.5. *Let $n \in \mathbb{N}$. Then n is a Giuga number if and only if*

$$\sum_{p|n} \frac{1}{p} - \prod_{p|n} \frac{1}{p}$$

is a positive integer.

For example, $n = 30$ is a Giuga number:

$$\frac{1}{2} + \frac{1}{3} + \frac{1}{5} - \frac{1}{30} = 1.$$

The following result, due to Giuga, combined the two types of numbers introduced earlier.

Theorem 13.9.6. *A composite number n satisfies $G_n \equiv -1 \bmod n$ if and only if it is both a Carmichael number and a Giuga number.*

Any counterexample to the Giuga-Agoh conjecture must be an odd square-free number with prime factorization $n = q_1 q_2 \cdots q_k$ such that

(1) $q_i \not\equiv 1 \bmod q_j$ for all i, j and

(2) $1/q_1 + 1/q_2 + \cdots + 1/q_k > 1$.

D. H. Bailey and J. M. Borwein [**35**] report that any counterexample must have at least 17168 digits.

Chapter 14

A Sample of Classical Polynomials: Legendre, Chebyshev, and Hermite

14.1. Introduction

There is a large variety of polynomials that have been studied in many different contexts. Many have appeared in problems in mathematical physics as solutions of differential equations. This chapter describes three such families. The reader will find a more systematic approach to these polynomials in the book by G. Andrews, R. Askey, and R. Roy [**18**].

14.2. Legendre polynomials

The construction of a polynomial vanishing at two points with prescribed multiplicity is elementary. Indeed, the solution is given by $(x-a)^n(x+b)^m$. The location of the roots may be moved to -1 and $+1$ via a linear change of variables to produce $(x-1)^n(x+1)^m$. This is a polynomial of degree $n+m$. The symmetric case, with roots of the same multiplicity, that is, $m=n$, becomes $(x^2-1)^n$. An interesting family of polynomials is obtained by reducing the degree to n by succesive differentiations. This leads to the first class of polynomials studied in this chapter.

Definition 14.2.1. The **Legendre polynomial** of order n is

$$P_n(x) := \frac{1}{2^n\, n!}\left(\frac{d}{dx}\right)^n (x^2-1)^n. \tag{14.2.1}$$

The expression (14.2.1) is called the **Rodrigues formula** for the Legendre polynomials.

The next exercise motivates the factor in the definition of P_n.

Exercise 14.2.2. Check that the polynomial P_n satisfies $P_n(1) = 1$.

Exercise 14.2.3. Express the polynomials $f_n(x)$ defined in (11.10.3) used to prove the irrationality of π in terms of the Legendre polynomials.

An explicit expression for $P_n(x)$. An elementary manipulation of (14.2.1) produces an explicit form of the Legendre polynomial.

Theorem 14.2.4. *The Legendre polynomial P_n is given by*

$$P_n(x) = \frac{1}{2^n}\sum_{j=0}^{n}\binom{n}{j}^2 (x-1)^j (x+1)^{n-j}. \tag{14.2.2}$$

Proof. The nth derivative of a product is computed by an expansion just as the binomial theorem

$$\begin{aligned}&\left(\frac{d}{dx}\right)^n [(x-1)^n(x+1)^n] \\ &\qquad = \sum_{j=0}^{n}\binom{n}{j}\left(\frac{d}{dx}\right)^j (x-1)^n \times \left(\frac{d}{dx}\right)^{n-j} (x+1)^n.\end{aligned}$$

Now use $\left(\frac{d}{du}\right)^j u^n = \frac{n!}{(n-j)!}u^{n-j}$ for $0 \leq j \leq n$ to obtain the result. □

Corollary 14.2.5. *The leading coefficient of $P_n(x)$ is $2^{-n}\binom{2n}{n}$.*

Proof. Expression (14.2.2) shows that the maximum degree is obtained by multiplying the leading coefficients of $(x-1)^j$ and $(x+1)^{n-j}$. Therefore, the leading coefficient of P_n is

$$\frac{1}{2^n}\sum_{j=0}^{n}\binom{n}{j}^2 = \frac{1}{2^n}\binom{2n}{n}. \tag{14.2.3}$$

This last identity is given in (5.2.18). □

Exercise 14.2.6. Give a proof of this corollary directly from the definition of P_n.

Exercise 14.2.7. Use Theorem 14.2.4 to prove that $P_n(1) = 1$ and $P_n(-1) = (-1)^n$.

Exercise 14.2.8. Verify that the Legendre polynomials can be written in terms of the hypergeometric function ${}_2F_1$ in the form

$$P_n(x) = {}_2F_1\left(-n, n+1; 1, \frac{1-x}{2}\right).$$

The function ${}_2F_1$ is defined in (5.5.3).

The issue of orthogonality. Given a set of linearly independent vectors $\{v_1, v_2, \ldots, v_m\}$ in $\mathbb{R}^n$, there is an elementary procedure for obtaining a set of orthogonal vectors $\{w_1, w_2, \ldots, w_m\}$ with the property that, for any $1 \le r \le m$, the vectors generated by $\{v_1, v_2, \ldots, v_r\}$ are the same as those generated by $\{w_1, w_2, \ldots, w_r\}$. This is the classical **Gram-Schmidt procedure**: start with

$$w_1 = v_1, \tag{14.2.4}$$

and continuing with $w_2 = v_2 - \alpha_{1,2}w_1$, where $\alpha_{1,2}$ is chosen so that w_2 is perpendicular to w_1. The process is repeated by forming

$$w_3 = v_3 - \alpha_{1,3}w_1 - \alpha_{2,3}w_2 \tag{14.2.5}$$

and determining the constants $\alpha_{1,3}$ and $\alpha_{2,3}$ using the condition that w_3 is orthogonal to w_1 and w_2. Observe that at each step in the process there is the choice of scaling the vector w_j.

The same procedure can be employed in the space of polynomials by replacing the vector product by

$$(f,g) := \int_a^b f(x)g(x)dx \tag{14.2.6}$$

and the length of a vector is now replaced by $\|f\| := (f,f)^{1/2}$.

Exercise 14.2.9. Apply the Gram-Schmidt process to the polynomials $\left\{x^j : j \geq 0\right\}$ on the interval $[-1,1]$ to obtain a family of orthogonal polynomials. The first five can be chosen to be

$$\begin{aligned} w_0(x) &= 1, \\ w_1(x) &= x, \\ w_2(x) &= 3x^2-1, \\ w_3(x) &= 5x^3-3x, \\ w_4(x) &= 35x^4-30x^2+3. \end{aligned}$$

Check that these polynomials agree, up to a multiple, with the Legendre polynomials.

The main result of this section is the orthogonality of the Legendre polynomials. The next exercises will be used in the proof.

Exercise 14.2.10. Prove that $P_n(x)$ is a polynomial of degree n with the same parity as n, that is, $P_{2n}(x)$ is even and $P_{2n+1}(x)$ is odd.

Exercise 14.2.11. Check that the polynomial

$$\left(\frac{d}{dx}\right)^j (x^2-1)^n \tag{14.2.7}$$

vanishes at $x = \pm 1$ if $j < n$.

The evaluation presented in the next proposition provides the value of the norm of the polynomial $P_n(x)$.

Proposition 14.2.12. *Let $n \in \mathbb{N}$. Then*

$$I_n := \int_{-1}^1 (1-x^2)^n \, dx = \frac{2^{2n+1}}{(2n+1)\binom{2n}{n}}. \tag{14.2.8}$$

Proof. Integrate by parts to produce the recurrence

$$I_{n+1} = \frac{2n+2}{2n+3} I_n. \tag{14.2.9}$$

Now define

$$J_n = \frac{2n+1}{2^{2n+1}} \binom{2n}{n} I_n. \tag{14.2.10}$$

Then (14.2.9) becomes $J_{n+1} = J_n$. The initial value $J_1 = 1$ gives the result. □

The next theorem shows that the Legendre polynomials are orthogonal on the interval $[-1, 1]$.

Theorem 14.2.13. *For n, $m \in \mathbb{N}_0$,*

$$\int_{-1}^{1} P_n(x) P_m(x)\, dx = \begin{cases} 0 & \textit{if } n \neq m, \\ \frac{2}{2n+1} & \textit{if } n = m. \end{cases} \tag{14.2.11}$$

Proof. Let

$$c_{n,m} := 2^{n+m} n! m! \int_{-1}^{1} P_n(x) P_m(x)\, dx, \tag{14.2.12}$$

and to compute

$$c_{n,m} = \int_{-1}^{1} \left(\frac{d}{dx}\right)^{n} (x^2-1)^n \left(\frac{d}{dx}\right)^{m} (x^2-1)^m\, dx,$$

integrate by parts and use Exercise 14.2.11 to check that the boundary terms vanish. This yields

$$c_{n,m} = -\int_{-1}^{1} \left(\frac{d}{dx}\right)^{n-1} (x^2-1)^n \left(\frac{d}{dx}\right)^{m+1} (x^2-1)^m\, dx.$$

Iterating this procedure gives

$$c_{n,m} = (-1)^j \int_{-1}^{1} \left(\frac{d}{dx}\right)^{n-j} (x^2-1)^n \left(\frac{d}{dx}\right)^{m+j} (x^2-1)^m\, dx.$$

Consider first the case $n \neq m$ and assume $n > m$. Now choose $j = n$ to obtain

$$c_{n,m} = (-1)^n \int_{-1}^{1} (x^2-1)^n \left(\frac{d}{dx}\right)^{m+n} (x^2-1)^m\, dx. \tag{14.2.13}$$

The integrand vanishes identically if $n > m+1$ because it is a polynomial of degree $2m$. In the case $n = m+1$, the original integrand is

$P_{m+1}(x)P_m(x)$ and Exercise 14.2.10 shows that this is an odd function, proving that its integral vanishes.

In the case $n = m$, equation (14.2.13) gives

$$\begin{aligned} c_{n,n} &= (-1)^n \int_{-1}^{1} (x^2-1)^n \left(\frac{d}{dx}\right)^{2n} (x^2-1)^n \, dx \\ &= (2n)! \int_{-1}^{1} (1-x^2)^n \, dx. \end{aligned}$$

The result now follows from Proposition 14.2.12. □

Recurrences. The general theory of orthogonal polynomials, expounded in [**18**], shows that any such sequence satisfies a three-term relation. The proof presented here appears in [**18**].

Theorem 14.2.14. *Assume* $\{p_n\}$ *is a collection of polynomials such that* $\deg p_n = n$ *and*

$$\langle p_n, p_m \rangle := \int_a^b p_n(x)p_m(x)w(x)\,dx = \begin{cases} h_n & \text{if } n = m, \\ 0 & \text{if } n \neq m \end{cases} \tag{14.2.14}$$

for a weight function $w(x)$. *Assume* $h_n \neq 0$. *Then* p_n *satisfies a three-term recurrence of the form*

$$p_{n+1}(x) = (A_n x + B_n)p_n(x) - C_n p_{n-1}(x), \quad \text{for } n \geq 1. \tag{14.2.15}$$

If the highest coefficient of $p_n(x)$ *is* k_n, *then*

$$A_n = \frac{k_{n+1}}{k_n} \quad \text{and} \quad C_n = \frac{A_n}{A_{n-1}} \frac{h_n}{h_{n-1}}. \tag{14.2.16}$$

Proof. Choose A_n so that $p_{n+1}(x) - A_n x p_n(x)$ is of degree n and write

$$p_{n+1}(x) - A_n x p_n(x) = \sum_{j=0}^{n} b_j p_j(x). \tag{14.2.17}$$

Match the leading coefficients to get the expression for A_n. The orthogonality of the polynomials shows that

$$\int_a^b p_n(x)Q(x)w(x)\,dx = 0 \tag{14.2.18}$$

for any polynomial Q of degree less than n. Multiply (14.2.17) by $p_k(x)w(x)$ and integrate over $[a, b]$ to conclude that $b_j = 0$ for $j < n-1$ (simply observe that $xp_k(x)$ has degree less than n). Therefore

$$p_{n+1}(x) = A_n x p_n(x) + b_{n-1}p_{n-1}(x) + b_n p_n(x). \tag{14.2.19}$$

The last identity comes from multiplying (14.2.19) by $p_{n-1}(x)w(x)$ and integrating. □

Exercise 14.2.15. Confirm the value of C_n. **Hint:** Use the identity

$$xp_{n-1}(x) = \frac{k_{n-1}}{k_n}p_n(x) + \sum_{k=0}^{n-1} d_k p_k(x). \tag{14.2.20}$$

Theorem 14.2.16. *The Legendre polynomials $P_n(x)$ satisfies*

$$P_{n+1}(x) = \frac{(2n+1)}{n+1}xP_n(x) - \frac{n}{n+1}P_{n-1}(x),$$

for $n \geq 2$.

Proof. The previous theorem shows the existence of a recurrence of the form

$$P_{n+1}(x) = (A_n x + B_n)P_n(x) - C_n P_{n-1}(x). \tag{14.2.21}$$

The normalization on the leading term gives $A_n = (2n+1)/(n+1)$. The parity of P_n, discussed in Exercise 14.2.10, shows that $B_n = 0$. The value $C_n = n/(n+1)$ comes from $h_n = 2/(2n+1)$. This is given in Theorem 14.2.13. □

Exercise 14.2.17. Use Theorem 14.2.16 at $x = 1$ and $x = -1$ to check that $P_n(1) = 1$ and $P_n(-1) = (-1)^n$.

Exercise 14.2.18. Use the recurrence (14.2.16) to obtain the expression

$$P_n(x) = \frac{1}{2^n}\sum_{k=0}^{\lfloor n/2 \rfloor} (-1)^k \binom{n}{k}\binom{2n-2k}{n} x^{n-2k}.$$

Exercise 14.2.19. The sequence of Legendre polynomials

$$\mathbb{L}_n := \{P_j(x) : 0 \leq r \leq n\}$$

has the property that $\deg(P_j) = j$. Any such sequence forms a basis of the space of polynomials of degree at most n. Prove the **inversion formula**

$$x^n = \sum_r \frac{(2r+1)\, n!}{2^{(n-r)/2}\left(\frac{n-r}{2}\right)!(n+r+1)!!} P_r(x) \tag{14.2.22}$$

where in the sum r starts at n and decreases by 2 ending at 1 or 0 depending on the parity of n. Compare this with Exercise 13.3.18.

The recurrence in Theorem 14.2.16, with the initial conditions $P_0(x) = 1$ and $P_1(x) = x$, determines the Legendre polynomials. The next proposition shows that the orthogonality of these polynomials follows simply from the recurrence.

Proposition 14.2.20. *Define polynomials $W_n(x)$ by*

$$W_{n+1}(x) = \frac{(2n+1)}{n+1} x W_n(x) - \frac{n}{n+1} W_{n-1}(x), \tag{14.2.23}$$

with $W_0(x) = 1$ and $W_1(x) = x$. Then the set of polynomials $\{W_n(x) : n \in \mathbb{N}_0\}$ forms an orthogonal sequence. In particular, for $n \neq m$,

$$I_{n,m} := \int_{-1}^{1} W_n(x) W_m(x)\, dx = 0. \tag{14.2.24}$$

Proof. The recurrence (14.2.23) gives

$$nI_{n,m} = (2n-1) \int_{-1}^{1} xW_{n-1}(x) W_m(x)\, dx - (n-1) I_{n-2,m}. \tag{14.2.25}$$

Replace n by m in (14.2.23) to obtain

$$xW_m(x) = \frac{m+1}{2m+1} W_{m+1}(x) + \frac{m}{2m+1} W_{m-1}(x),$$

and then (14.2.25) gives

$$I_{n,m} = \frac{(2n-1)(m+1)}{n(2m+1)} I_{n-1,m+1} + \frac{(2n-1)m}{(2m+1)n} I_{n-1,m-1} - \frac{n-1}{n} I_{n-2,m},$$

for $n \geq 2$. The orthogonality (14.2.24) follows by induction on n. In order to check that $W_n(x)$ is the Legendre polynomial, it remains to verify that the leading coefficient of $W_n(x)$ is $2^{-n}\binom{2n}{n}$. This follows directly from the recurrence (14.2.23) as only one term on the right contributes to the calculation of the leading coefficient. □

Legendre's differential equation. Legendre polynomials also appear from one of the basic equations of mathematical physics. **Laplace's equation** states that

$$\Delta u = \sum_{j=1}^{n} \frac{\partial^2 u}{\partial x_j^2} = 0.$$

This equation leads to classical differential equations by considering special coordinate systems. The **spherical coordinates** (r, θ, ϕ) of a point $P = (x, y, z)$ in $\mathbb{R}^3$ are defined in the following form: the **radius** r is the distance from P to the origin $(0, 0, 0)$; the **azimuthal angle** θ is the angle of the projection of P to the xy-plane measured from the x-axis, and the **polar angle** ϕ is the angle from the positive part of the z-axis to the point P.

Exercise 14.2.21. Prove the formulas for changing coordinates:

$$\begin{aligned} x &= r\cos\theta\sin\phi, \\ y &= r\sin\theta\sin\phi, \\ z &= r\cos\phi. \end{aligned}$$

Derive formulas for (r, θ, ϕ) in terms of (x, y, z) by inverting the previous set.

Exercise 14.2.22. Write down Laplace's equation in spherical coordinates:

$$\Delta u = \frac{1}{r^2}\frac{\partial}{\partial r}\left(r^2 \frac{\partial u}{\partial r}\right) + \frac{1}{r^2 \sin^2\phi}\frac{\partial^2 u}{\partial \theta^2} + \frac{1}{r^2\sin\phi}\frac{\partial}{\partial \phi}\left(\sin\phi\,\frac{\partial u}{\partial \phi}\right).$$

Now assume that the solution u is independent of the angle θ. Then Laplace's equation becomes

$$\frac{\partial}{\partial r}\left(r^2 \frac{\partial u}{\partial r}\right) + \frac{1}{\sin\phi}\frac{\partial}{\partial \phi}\left(\sin\phi\,\frac{\partial u}{\partial \phi}\right) = 0. \tag{14.2.26}$$

Exercise 14.2.23. Make the change of variables $x = \cos\phi$ and show that (14.2.26) becomes

$$\frac{\partial}{\partial r}\left(r^2 \frac{\partial u}{\partial r}\right) + \frac{\partial}{\partial x}\left((1 - x^2)\frac{\partial u}{\partial x}\right). \tag{14.2.27}$$

Exercise 14.2.24. Now look for a special solution of the form

$$u(x,r) = \sum_{n=0}^{\infty} r^n Y_n(x)$$

for some function $Y_n(x)$. Substitute this form of $u(x,r)$ in (14.2.27) to prove that Y_n satisfies the equation

$$(1-x^2)Y_n''(x) - 2xY_n'(x) + n(n+1)Y_n(x) = 0. \tag{14.2.28}$$

Now use the recurrence for Legendre polynomials to show that the polynomials P_n satisfy

$$P_{n+1}'(x) = xP_n'(x) + (n+1)P_n(x)$$

and

$$P_n'(x) = xP_{n+1}'(x) - (n+1)P_{n+1}(x).$$

Confirm that $y = P_n(x)$ solves **Legendre's differential equation**

$$(1-x^2)y''(x) - 2xy'(x) + n(n+1)y(x) = 0. \tag{14.2.29}$$

By choosing Y_0 and Y_1, show that $Y_n(x) = P_n(x)$ for all $n \in \mathbb{N}$.

Integrals involving Legendre polynomials. The orthogonality relations

$$\int_{-1}^{1} P_n(x)P_m(x)\,dx = \begin{cases} 0 & \text{if } n \neq m, \\ \frac{2}{2n+1} & \text{if } n = m \end{cases}$$

provide definite integrals involving Legendre polynomials. The next example appears in C. C. Grosjean [**150**] and it relates the Legendre polynomials and the harmonic numbers $H_n = 1 + \frac{1}{2} + \cdots + \frac{1}{n}$ from Section 11.11. The papers by C. C. Grosjean [**150, 151, 152, 153**] really constitute a nice book on the evaluation of integrals.

Theorem 14.2.25. *Let $n \in \mathbb{N}$. Then*

$$\int_{-1}^{1} \frac{1-P_n(x)}{1-x}\,dx = 2H_n. \tag{14.2.30}$$

Proof. Introduce the notation

$$I_n := \int_{-1}^{1} \frac{1-P_n(x)}{1-x}\,dx, \tag{14.2.31}$$

and observe that

$$I_{n+1} - I_n = \int_{-1}^{1} \frac{P_n(x) - P_{n+1}(x)}{1-x}\, dx. \tag{14.2.32}$$

It is now shown that the integrand in (14.2.32) is a perfect derivative. To establish this, add the identities in Exercise 14.2.24 to produce

$$P'_{n+1}(x) + P'_n(x) = x\left(P'_n(x) + P'_{n+1}(x)\right) + (n+1)\left(P_n(x) - P_{n+1}(x)\right);$$

therefore

$$\frac{P_n(x) - P_{n+1}(x)}{1-x} = \frac{1}{n+1}\left(P'_n(x) + P'_{n+1}(x)\right). \tag{14.2.33}$$

Then, integrating (14.2.32) and using $P_n(1) = 1$ and $P_n(-1) = (-1)^n$ gives

$$I_{n+1} - I_n = \frac{1}{n+1}\left(2 - (-1)^n - (-1)^{n+1}\right) = \frac{2}{n+1}. \tag{14.2.34}$$

Now sum from 0 to n to obtain the result. □

Exercise 14.2.26. Let $n \in \mathbb{N}$ and let $0 \leq m \leq n-1$. Then

$$\int_{-1}^{1} \frac{1 - P_n(x)}{1-x} P_m(x)\, dx = 2(H_n - H_m). \tag{14.2.35}$$

Exercise 14.2.27. The value $P_n(1) = 1$, given in Exercise 14.2.17, shows that

$$P_n^{\#}(x) := \frac{1 - P_n(x)}{1-x} \tag{14.2.36}$$

is a polynomial in x of degree $n-1$. Prove that

$$P_n^{\#}(x) = \sum_{k=0}^{n-1} (H_n - H_k)(2k+1)P_k(x). \tag{14.2.37}$$

Definition 14.2.28. The **shifted Legendre polynomials** are defined by

$$P_n^*(x) = P_n(2x-1). \tag{14.2.38}$$

The first few examples are given by

$$P_0^*(x) = 1, \quad P_1^*(x) = 2x - 1, \quad P_2^*(x) = 6x^2 - 6x + 1. \tag{14.2.39}$$

The next result is due to J. L. Blue [**56**]. It appeared in the context of finding a family of orthogonal polynomials that was numerically stable for an integration algorithm.

Theorem 14.2.29. *Let $n \geq 1$. Then*

$$\int_0^1 P_n^*(x) \ln \frac{1}{x}\, dx = \frac{(-1)^n}{n(n+1)}. \tag{14.2.40}$$

Proof. The recurrence (14.2.16) becomes

$$(n+1)P_{n+1}^*(x) = (2n+1)(2x-1)P_n^*(x) - nP_{n-1}^*(x), \quad \text{for } n \geq 2.$$

Multiply by $\ln(1/x)$ and integrate to produce

$$\begin{aligned}(n+1)\int_0^1 P_{n+1}^*(x) \ln \frac{1}{x}\, dx = (2n+1) &\int_0^1 (2x-1)P_n^*(x) \ln \frac{1}{x}\, dx \\ &- n\int_0^1 P_{n-1}^*(x) \ln \frac{1}{x}\, dx.\end{aligned}$$

Introduce the notation

$$\nu_n = \int_0^1 P_n^*(x) \ln \frac{1}{x}\, dx \quad \text{and} \quad \mu_n = \int_0^1 (2x-1)P_n^*(x) \ln \frac{1}{x}\, dx,$$

to write the previous relation as

$$(n+1)\nu_{n+1} = (2n+1)\mu_n - n\nu_{n-1}. \tag{14.2.41}$$

Exercise 14.2.30. Integrate by parts the integral μ_n to obtain

$$\mu_n = -\frac{1}{2} - \frac{n}{2}\mu_n + \frac{n}{2}\nu_{n-1} - \frac{1}{2}\int_0^1 x(x-2)\left[\frac{d}{dx}P_n^*(x)\right] dx.$$

The last integral in Exercise 14.2.30 is now computed by parts to obtain

$$\int_0^1 x(x-2)\left[\frac{d}{dx}P_n^*(x)\right] dx = -2\int_0^1 (x-1)P_n^*(x)\, dx = 0$$

for $n \geq 2$, by orthogonality of the Legendre polynomials. It follows that

$$\mu_n = \frac{n}{n+1}\nu_{n-1}. \tag{14.2.42}$$

Substitute this in (14.2.41) to obtain

$$\nu_{n+1} = \frac{n(n-1)}{(n+1)(n+2)}\nu_{n-1}. \tag{14.2.43}$$

The result follows by induction starting at $\nu_0 = 1$ and $\nu_1 = -\frac{1}{2}$. □

Exercise 14.2.31. Prove the identity

$$\int_x^1 P_n(t)\,dt = \frac{(1-x^2)}{n(n+1)}\frac{d}{dx}P_n(x).$$

The generating function. The next goal is to establish an expression for the generating function of the Legendre polynomials. This is the special function $u(x,r)$ given in Exercise 14.2.24. (The radial variable r has been replaced by t.)

Theorem 14.2.32. *The generating function of the Legendre polynomials is given by*

$$\sum_{n=0}^{\infty} P_n(x)t^n = \frac{1}{\sqrt{1-2xt+t^2}}. \tag{14.2.44}$$

Proof. Denote by $L(x,t)$ the left-hand side of (14.2.44). The recurrence (14.2.16) is multiplied by t^n to obtain

$$(n+1)P_n(x)t^n = (2n+1)xP_n(x)t^n - nP_{n-1}(x)t^n \tag{14.2.45}$$

and summing over n gives

$$(t^2-2xt+1)\frac{\partial L}{\partial t} = (x-t)L, \tag{14.2.46}$$

which yields the result after integration. The implied constant of integration is determined by the condition $P_n(1)=1$. □

Exercise 14.2.33. Use the generating function of the Legendre polynomials to verify the identity

$$\sum_{n=0}^{\infty}(2n+1)P_n(x)t^n = \frac{1-t^2}{(1-2xt+t^2)^{3/2}}.$$

Relations to binomial sums. Chapter 5 contains a proof that the sum

$$L_3(n) = \sum_{k=0}^{n}\binom{n}{k}^3 \tag{14.2.47}$$

cannot be expressed as a hypergeometric function of n. A relation between $L_3(n)$ and the Legendre polynomials is established now. The author found the first result as a problem proposed by L. Carlitz and solved by Chih-Yi Yang.

Theorem 14.2.34. *The sum $L_3(n)$ is the coefficient of x^n in*

$$Z_3(x) = (1-x^2)^n P_n\left(\frac{1+x}{1-x}\right).$$

Proof. The expression (14.2.2) is written as

$$P_n(x) = \frac{(x+1)^n}{2^n}\sum_{j=0}^{n}\binom{n}{j}^2\left(\frac{x-1}{x+1}\right)^j. \tag{14.2.48}$$

Therefore

$$(1-x^2)^n P_n\left(\frac{1+x}{1-x}\right) = (1+x)^n\sum_{j=0}^{n}\binom{n}{j}^2 x^j. \tag{14.2.49}$$

The result is obtained by expanding this last product. □

Exercise 14.2.35. Prove that the coefficient of x^n in the polynomial

$$Z_4(x) = (1-x)^{2n}P_n^2\left(\frac{1+x}{1-x}\right) \tag{14.2.50}$$

is

$$L_4(n) = \sum_{j=0}^{n}\binom{n}{j}^4. \tag{14.2.51}$$

14.3. Chebyshev polynomials

The second family of polynomials considered here came from Chapter 12. Two sequences of polynomials that express the value of $\sin mx$ and $\cos mx$ in terms of $\sin x$ and $\cos x$ were introduced in Corollary 12.5.4. The treatment becomes more unified when only the variable $t = \cos x$ is employed.

Definition 14.3.1. The **Chebyshev polynomial of the first kind** T_n is defined by the relation

$$\cos nx = T_n(\cos x). \tag{14.3.1}$$

The **Chebyshev polynomial of the second kind** U_n is

$$\frac{\sin(n+1)x}{\sin x} = U_n(\cos x). \tag{14.3.2}$$

Note 14.3.2. Observe the similarity in the definition of T_n to the rational functions R_n introduced in Example 8.1.6. The polynomials T_n satisfy the commutation relation $T_m \circ T_n = T_n \circ T_m$ for the same reason as given in Exercise 8.1.7.

Exercise 14.3.3. Verify that T_n satisfies the **Chebyshev differential equation**

$$(1-x^2)y'' - xy' + n^2 y = 0. \tag{14.3.3}$$

Hint: The function $w = \cos nx$ satisfies $w'' + n^2 w = 0$. Now write this in terms of the variable $t = \cos x$.

Note 14.3.4. The polynomial T_n is exactly R_n in (12.5.3). The relation between U_n and S_n in (12.5.4) is given by

$$U_m(t) = \frac{1}{\sqrt{1-t^2}} S_{m+1}(\sqrt{1-t^2}), \quad \text{for } m \text{ even} \tag{14.3.4}$$

and

$$U_m(t) = \frac{t}{\sqrt{1-t^2}} S_{m+1}(\sqrt{1-t^2}), \quad \text{for } m \text{ odd.} \tag{14.3.5}$$

Exercise 14.3.5. Check the details.

A recurrence. The next exercise gives a recurrence for the functions T_n and U_n. A consequence of it is that T_n and U_n are polynomials in t with integer coefficients.

Exercise 14.3.6. Show that T_n and U_n satisfy the same recurrence

$$f_n(t) - 2tf_{n-1}(t) + f_{n-2}(t) = 0. \tag{14.3.6}$$

The initial conditions are $T_0(t) = 1$ and $T_1(t) = t$ for the polynomials of the first kind and they are $U_0(t) = 1$ and $U_1(t) = 2t$ for those of the second kind. The recurrence (14.3.6) includes both (12.5.5) and (12.5.6) at once.

The orthogonality property. The next property discussed here is the orthogonality of the Chebyshev polynomials. This comes from the elementary identity

$$\int_0^\pi \cos nx \, \cos mx \, dx = \begin{cases} 0 & \text{if } m \neq n, \\ \pi & \text{if } m = n = 0, \\ \pi/2 & \text{if } m = n \neq 0 \end{cases} \tag{14.3.7}$$

and the change of variable $t = \cos x$ produces

$$\int_{-1}^{1} \frac{T_n(t)T_m(t)}{\sqrt{1-t^2}}\,dt = \begin{cases} 0 & \text{if } m \neq n, \\ \pi & \text{if } m = n = 0, \\ \pi/2 & \text{if } m = n \neq 0. \end{cases} \tag{14.3.8}$$

This is the **orthogonality relation** for the Chebyshev polynomials.

Exercise 14.3.7. Check that the leading term of T_n is 2^{n-1}. Also verify the value $T_n(1) = 1$.

Note 14.3.8. The recurrence (14.3.6) is consistent with the general recurrence for orthogonal polynomials given in Theorem 14.2.14. Indeed, using Exercise 14.3.7, this recurrence becomes

$$T_{n+1}(x) = (2x + B_n)T_n(x) - T_{n-1}(x).$$

The fact that $B_n = 0$ comes from replacing $x = 1$ and using Exercise 14.3.7.

Exercise 14.3.9. Use the recurrence (14.3.6) to verify that the generating function for Chebyshev polynomials is given by

$$\sum_{n=0}^{\infty} T_n(x)t^n = \frac{1 - xt}{1 - 2xt + t^2}. \tag{14.3.9}$$

Exercise 14.3.10. Verify that the Chebyshev polynomials can be written in terms of the hypergeometric function ${}_2F_1$, defined in (5.5.3), in the form

$$T_n(x) = {}_2F_1\left(-n, n; \frac{1}{2}, \frac{1-x}{2}\right).$$

Polynomial interpolation. The question of polynomial interpolation was addressed in Exercise 4.2.7. Given a collection of n points $\{(x_i, y_i) : 1 \leq i \leq n\}$, with $x_i \in [-1, 1]$ and $x_i \neq x_j$ for $i \neq j$, there is a unique polynomial J_{n-1} of degree n such that $J_{n-1}(x_i) = y_i$. A different type of interpolation question, connected to the Chebyshev polynomials, is described next.

Given a function f defined on $[-1, 1]$ and given $n \in \mathbb{N}$, the question is how to choose a collection of n points $\{x_i : 1 \leq i \leq n\}$ in order to minimize the error $|f(x) - P_{n-1}(x)|$. The following theorem provides the answer.

Theorem 14.3.11. *Let $n \in \mathbb{N}$ and let $f : [-1,1] \mapsto \mathbb{R}$ be a continuous functions. Let $\{x_i : 1 \leq i \leq n\}$ be a collection of n points. Then the error term*

$$\text{Max}\,\{|f(x) - P_{n-1}(x)| : -1 \leq x \leq 1\}$$

is minimal if $x_i = \cos\left(\frac{2i-1}{2n}\pi\right)$ for $1 \leq i \leq n$. These are the ***Chebyshev nodes****. They satisfy $T_n(x_i) = 0$.*

The reader will find a complete discussion of this result in the text by R. L. Burden and D. Faires [**85**].

14.4. Hermite polynomials

The last class of polynomials described in this text is the **Hermite polynomials**. These can be defined by a Rodrigues formula as was done to introduce the Legendre polynomials or by an orthogonality process that was employed to present the Chebyshev polynomials. In order to show the reader that there are many ways to start, these polynomials are introduced by their exponential generating function.

Definition 14.4.1. The Hermite polynomials $H_n(x)$ are defined by the identity

$$e^{2xt-t^2} = \sum_{n=0}^{\infty} \frac{H_n(x)\,t^n}{n!}. \tag{14.4.1}$$

It is unclear from this definition that $H_n(x)$ is a polynomial. This is verified first.

Proposition 14.4.2. *The function $H_n(x)$ is a polynomial in x of degree n.*

Proof. Differentiate the generating function with respect to x to produce

$$2te^{2xt-t^2} = \sum_{n=0}^{\infty} \frac{H_n'(x)t^n}{n!}.$$

Then (14.4.1) gives $H_n'(x) = 2nH_{n-1}(x)$. The result now follows by induction starting with the value $H_0(x) = 1$, obtained by setting $t = 0$ in (14.4.1). □

Corollary 14.4.3. *The Hermite polynomials $H_n(x)$ satisfy the recurrence*

$$H'_n(x) = 2nH_{n-1}(x). \tag{14.4.2}$$

Exercise 14.4.4. Check that the leading coefficient of $H_n(x)$ is 2^n.

The next step is to produce a recurrence for $H_n(x)$ that does not involve derivatives.

Theorem 14.4.5. *The Hermite polynomials satisfy the three-term recurrence*

$$H_{n+1}(x) = 2xH_n(x) - 2nH_{n-1}(x).$$

Proof. Differentiate the generating function with respect to t to produce

$$(2x-2t)e^{2xt-t^2} = \sum_{n=0}^{\infty} \frac{H_{n+1}(x)t^n}{n!}.$$

The result now follows by using (14.4.1) on the left-hand side of the previous identity. □

Rodrigues's formula and the orthogonality relation. The next item is to establish a Rodrigues formula for the Hermite polynomial. The original definition will appear to be unmotivated, although the appearance of the Gaussian kernel in the generating function gives a hint of what is coming up. The orthogonality relations established in the next section provide a second explanation of why the Gaussian kernel is employed here.

Define the function

$$Y_n(x) = e^{x^2}\left(\frac{d}{dx}\right)^n e^{-x^2}. \tag{14.4.3}$$

Then

$$Y_{n+1}(x) = e^{x^2}\frac{d}{dx}\left[e^{-x^2}Y_n(x)\right]$$

produces

$$Y_{n+1}(x) = \frac{d}{dx}Y_n(x) - 2xY_n(x).$$

Define the quotient

$$q_n(x) = (-1)^n\frac{Y_n(x)}{H_n(x)}. \tag{14.4.4}$$

The computation

$$\begin{aligned}
(-1)^n q_n'(x) &= \frac{Y_n'(x)H_n(x) - Y_n(x)H_n'(x)}{H_n^2(x)} \\
&= \frac{(Y_{n+1}(x) + 2xY_n(x))H_n(x) - Y_n(x)\cdot 2nH_{n-1}(x)}{H_n^2(x)} \\
&= \frac{Y_{n+1}(x)H_n(x) + Y_n(x)(2xH_n(x) - 2nH_{n-1}(x))}{H_n^2(x)} \\
&= \frac{Y_{n+1}(x)H_n(x) + Y_n(x)H_{n+1}(x)}{H_n^2(x)},
\end{aligned}$$

leads to

$$q_n'(x) = (q_n(x) - q_{n+1}(x))\,\frac{H_{n+1}(x)}{H_n(x)}. \tag{14.4.5}$$

Assume, as inductive hypoyhesis, that $q_n(x) \equiv 1$. Then (14.4.5) gives

$$0 = (1 - q_{n+1}(x))H_{n+1}(x),$$

which implies $q_{n+1}(x) \equiv 1$.

Theorem 14.4.6. *The Hermite polynomials have a Rodrigues formula*

$$H_n(x) = (-1)^n e^{x^2}\left(\frac{d}{dx}\right)^n e^{-x^2}.$$

The previous result gives a direct proof of the orthogonality relations for the Hermite polynomials.

Theorem 14.4.7. *The Hermite polynomials satisfy the orthogonality relations*

$$\int_{-\infty}^{\infty} e^{-x^2} H_n(x)H_m(x)\,dx = \begin{cases} 2^n n!\,\sqrt{\pi} & \textit{if } n = m, \\ 0 & \textit{if } n \neq m. \end{cases}$$

Proof. Theorem 14.4.6 gives

$$\begin{aligned}
Q_n &:= (-1)^n \int_{-\infty}^{\infty} e^{-x^2} H_n(x)H_m(x)\,dx \\
&= \int_{-\infty}^{\infty} \left(\frac{d}{dx}\right)^n e^{-x^2} \times H_m(x)\,dx
\end{aligned}$$

and integration by parts produces

$$Q_n = \left(\frac{d}{dx}\right)^{n-1} e^{-x^2} \times \frac{d}{dx}H_m(x)\Big|_{-\infty}^{\infty} \\ - \int_{-\infty}^{\infty} \left(\frac{d}{dx}\right)^{n-1} e^{-x^2} \times \frac{d}{dx}H_m(x)\,dx.$$

The boundary terms vanish, leading to

$$Q_n = -\int_{-\infty}^{\infty} \left(\frac{d}{dx}\right)^{n-1} e^{-x^2} \times \frac{d}{dx}H_m(x)\,dx.$$

Iteration of this procedure shows that

$$Q_n = (-1)^j \int_{-\infty}^{\infty} \left(\frac{d}{dx}\right)^{n-j} e^{-x^2} \times \left(\frac{d}{dx}\right)^{j} H_m(x)\,dx.$$

If $n \neq m$, assume that $n > m$. Now choose j in the range $m < j \leq n$ to see that Q_n must be zero because $H_m(x)$ is of degree m.

In the case $n = m$, the previous relation gives

$$Q_n = (-1)^n \int_{-\infty}^{\infty} e^{-x^2} \times \left(\frac{d}{dx}\right)^{n} H_n(x)\,dx.$$

Exercise 14.4.4 shows that the polynomial $H_n(x)$ has leading coefficient 2^n. Therefore,

$$Q_n = (-1)^n 2^n n! \int_{-\infty}^{\infty} e^{-x^2}\,dx = (-1)^n 2^n n!\,\sqrt{\pi}. \tag{14.4.6}$$

The proof is complete. □

Note 14.4.8. The last step of the proof employs the value of the **normal integral**

$$\int_{-\infty}^{\infty} e^{-x^2}\,dx = \sqrt{\pi}. \tag{14.4.7}$$

The reader will find a variety of proofs of this formula in the book by G. Boros and V. Moll [**65**].

Hermite's differential equation. An immediate consequence of the recurrences given here for the Hermite polynomials is that they satisfy the **Hermite differential equation**

$$y'' - 2xy' + 2ny = 0.$$

In order to verify this, differentiate the relation $H_n' = 2nH_{n-1}$ to obtain

$$H_n'' = 2nH_{n-1}' = 4n(n-1)H_{n-2}. \tag{14.4.8}$$

Theorem 14.4.5 is now used to write (14.4.8) as

$$H_n'' = 2n\,(2xH_{n-1} - H_n) = 4nxH_{n-1} - 2nH_n.$$

The result is obtained by replacing $2nH_{n-1}$ by H_n' in the first term on the right-hand side.

Exercise 14.4.9. This exercise presents an alternative proof of the orthogonality relation for Hermite polynomials. For $j \in \mathbb{N} \cup \{0\}$, define

$$u_j(x) = e^{-x^2/2}H_j(x).$$

Check that u_j satisfies $u_j'' + (2j+1-x^2)u_j = 0$. Multiply the equation for $j = n$ by u_m and the one for $j = m$ by u_n. Then subtract to produce

$$u_m u_n'' - u_n u_m'' = 2(m-n)u_n u_m.$$

Now integrate over $\mathbb{R}$ to conclude the result for $n \neq m$.

Exercise 14.4.10. Use the Hermite differential equation to obtain a recurrence for the coefficients of the polynomial $H_n(x)$. Solve the recurrence and prove the explicit formula

$$H_n(x) = \sum_{j=0}^{\lfloor n/2 \rfloor} \frac{(-1)^j n!}{j!(n-2j)!}(2x)^{n-2j}. \tag{14.4.9}$$

Conclude that $H_n(-x) = (-1)^n H_n(x)$.

The quantum harmonic oscillator. The Hermite polynomials appear in relation to the quantum analog of the classical harmonic oscillator. The starting point is the **Schrödinger equation**

$$\psi'' + \frac{2m}{\hbar^2}\left(E - V(y)\right)\psi = 0. \tag{14.4.10}$$

The special case of $V(y) = y^2$ is considered here.

Exercise 14.4.11. Check that (14.4.10) can be scaled to the form

$$\psi'' - x^2\psi = \beta\psi. \tag{14.4.11}$$

Describe β in terms of the original parameters.

Exercise 14.4.12. Define $\psi_*(x) = e^{-x^2/2}$. Check that

$$\psi_*'' - x^2\psi_* = -\psi_*.$$

The **method of variations of parameters** is now employed to look for a solution of (14.4.11) in the form $\psi(x) = \psi_*(x)H(x)$. This produces

$$H'' - 2xH' + (\beta - 1)H = 0.$$

The choice of $\beta = 2n + 1$ gives the Hermite differential equation.

Note 14.4.13. A very nice description of the basic properties of Hermite polynomials can be found in C. T. Aravnis [**28**].

An appearance of Hermite polynomials in combinatorics. Consider a set A with an even number of elements, say $|A| = 2s$, and a partition of A into k subsets B_i of cardinality $|B_i| = n_i$. A **matching** is an arrangement of the elements of A into s pairs $\{a_j,\, a_k\}$. The matching is called **homogeneous** if a_j, a_k are in the same set B_i and it is called **heterogeneous** if not. For a matching $\{A, B_i\}$ let

$$\alpha(A; B_i) = \text{the number of homogeneous pairs.}$$

The paper by R. Azor, J. Gillis, and J. D. Victor [**32**] contains a study of the quantities

$$\begin{aligned} E(n_1, \ldots, n_k) &= |(A; B_i) : 0 < \alpha(A; B_i) \equiv 0 \bmod 2|, \\ \Omega(n_1, \ldots, n_k) &= |(A; B_i) : \alpha(A; B_i) \equiv 1 \bmod 2|, \\ P(n_1, \ldots, n_k) &= |(A; B_i) : \alpha(A; B_i) = 0|. \end{aligned}$$

That is, E counts the number of matchings with an even number of homogeneous pairs, Ω counts those with an odd number, and P counts those without homogeneous pairs.

Define the integral

$$I(n_1, \ldots, n_k) = \int_{-\infty}^{\infty} e^{-x^2} \prod_{i=1}^{k} H_{n_i}(x)\, dx.$$

The result of [**32**] is stated next.

Theorem 14.4.14. *With the notation introduced above,*

$$P(n_1, \ldots, n_k) = \frac{1}{2^s \sqrt{\pi}} I(n_1, \ldots, n_k)$$

and

$$E(n_1, \ldots, n_k) - \Omega(n_1, \ldots, n_k) = \sqrt{\frac{2}{\pi}} \int_{-\infty}^{\infty} e^{-2x^2} \prod_{i=1}^{k} H_{n_i}(x)\, dx.$$

Exercise 14.4.15. Let n_1, n_2, $n_3 \in \mathbb{N}$ with $n_1 + n_2 + n_3 = 2s$. Prove that

$$\int_{-\infty}^{\infty} e^{-x^2} H_{n_1}(x)\, H_{n_2}(x)\, H_{n_3}(x)\, dx = \frac{2^s \sqrt{\pi}\; n_1!\, n_2!\, n_3!}{(s - n_1)!\, (s - n_2)!\, (s - n_3)!}.$$

Compare this with Theorem 14.4.7.

Note 14.4.16. There is a large literature of relations between orthogonal polynomials and combinatorics. The reader will find an expression for derangements in terms of Laguerre polynomials in S. Even and J. Gillis [**123**]. More information can be found in the paper by I. Gessel [**134**].

Chapter 15

Landen Transformations

15.1. Introduction

The transformation of variables plays an important role in the theory of definite integrals. From the beginning, the reader has been exposed to some common changes of variables, motivated mainly by the fact that they work. For example, the basic knowledge of trigonometry presented in Chapter 12 shows that confronted with a problem of the type

$$I(a,b) = \int_a^b \frac{dt}{\sqrt{1-t^2}}, \tag{15.1.1}$$

the change of variables

$$t = \sin x \tag{15.1.2}$$

leads to a simpler form of the integral.

Naturally, this change of variable, presented in the form

$$x = \sin^{-1} t \tag{15.1.3}$$

manifests the new variable of integration as the inverse of a transcendental function.

A different type of map that leaves certain integrals invariant is defined next.

Definition 15.1.1. A **Landen transformation** for an integral

$$I = \int_{x_0}^{x_1} f(x; \mathbf{p})\, dx, \tag{15.1.4}$$

which depends on a set of parameters $\mathbf{p}$, is a map Φ, defined on the parameters of I, such that

$$\int_{x_0}^{x_1} f(x; \mathbf{p})\, dx = \int_{\Phi(x_0)}^{\Phi(x_1)} f(x; \Phi(\mathbf{p}))\, dx. \tag{15.1.5}$$

Example 15.1.2. The classical example of a Landen transformation is given by

$$\mathfrak{E}(a, b) = \left(\frac{a+b}{2}, \sqrt{ab} \right), \tag{15.1.6}$$

which preserves the **elliptic integral**

$$G(a, b) = \int_0^{\pi/2} \frac{dx}{\sqrt{a^2 \cos^2 x + b^2 \sin^2 x}}, \tag{15.1.7}$$

that is,

$$G(a, b) = G\left(\frac{a+b}{2}, \sqrt{ab} \right). \tag{15.1.8}$$

It turns out that the sequence (a_n, b_n) defined inductively by

$$(a_n, b_n) = \mathfrak{E}(a_{n-1}, b_{n-1}) \tag{15.1.9}$$

with $(a_0, b_0) = (a, b)$ has the property that

$$\lim_{n\to\infty} a_n = \lim_{n\to\infty} b_n. \tag{15.1.10}$$

This limit is the **arithmetic-geometric mean** of a and b, denoted by $\text{AGM}(a, b)$. The invariance of the elliptic integral shows that

$$G(a, b) = \frac{\pi}{2\text{AGM}(a, b)}. \tag{15.1.11}$$

This may be used to compute the elliptic integral $G(a, b)$ by iteration.

This chapter discusses Landen transformations in the case when the integrand is a rational function. The idea is to produce an appropriate change of variables that leaves the rational integral invariant. The special example

$$x = R_2(t) = \frac{t^2 - 1}{2t} \tag{15.1.12}$$

appearing in Example 8.1.6 leads to the simplest nontrivial class of Landen transformations.

This chapter contains details of the effect of this map on two special kinds of integrands. The first one establishes the formula

$$\int_0^\infty \frac{dx}{(x^4+2ax^2+1)^{m+1}} = \frac{\pi}{2}\frac{1}{[2(1+a)]^{m+1/2}}P_m(a), \tag{15.1.13}$$

where $P_m(a)$ is a polynomial in a.

Warning: The symbol P_m has been used to denote other polynomials in this text, for instance the Legendre polynomials. In this chapter, this refers only to the polynomial (15.4.16).

Many properties of its coefficients are presented (not proved) in this chapter. The second example provides a Landen transformation for the integral

$$U_6(a,b;c,d,e) = \int_0^\infty \frac{cx^4+dx^2+e}{x^6+ax^4+bx^2+1}\,dx, \tag{15.1.14}$$

which leads to an interesting nonlinear transformation.

15.2. An elementary example

The goal of this section is to establish the following result.

Theorem 15.2.1. *Let f be a function, with finite integral over $\mathbb{R}$. Define*

$$f_\pm(x) = f(x+\sqrt{x^2+1}) \pm f(x-\sqrt{x^2+1}) \tag{15.2.1}$$

and

$$\mathfrak{L}(f)(x) = f_+(x) + \frac{xf_-(x)}{\sqrt{x^2+1}}. \tag{15.2.2}$$

Then

$$\int_{-\infty}^\infty f(t)\,dt = \int_{-\infty}^\infty \mathfrak{L}(f)(x)\,dx. \tag{15.2.3}$$

Proof. The map $x = R_2(t)$ has two branches separated by the pole at $t=0$. The inverses are given by

$$t = x \pm \sqrt{x^2+1}. \tag{15.2.4}$$

Each branch maps a half-line onto $\mathbb{R}$. Therefore it is natural to consider integrals over the whole line. The change of variables (15.2.4) leads to

$$\begin{aligned} I &= \int_{-\infty}^{\infty} f(t)\,dt \\ &= \int_{-\infty}^{0} f(t)\,dt + \int_{0}^{\infty} f(t)\,dt \\ &= \int_{-\infty}^{\infty} f(x-\sqrt{x^2+1})\left(1-\frac{x}{\sqrt{x^2+1}}\right)dx \\ &\qquad + \int_{-\infty}^{\infty} f(x+\sqrt{x^2+1})\left(1+\frac{x}{\sqrt{x^2+1}}\right)dx. \end{aligned}$$

Now collect terms to obtain the claim. □

Example 15.2.2. Take $f(t) = 1/(t^2+1)$. Then $\mathfrak{L}(f)(x) = f(x)$ and the function f is fixed by $\mathfrak{L}$. Now take $f(t) = 1/(t^2+2)$ to obtain

$$\mathfrak{L}(f)(x) = \frac{6}{8x^2+9}. \tag{15.2.5}$$

The theorem gives the elementary identity

$$\int_{-\infty}^{\infty} \frac{dx}{x^2+2} = \int_{-\infty}^{\infty} \frac{6\,dx}{8x^2+9}. \tag{15.2.6}$$

Both sides evaluate to $\pi/\sqrt{2}$.

Example 15.2.3. The function $f(t) = \dfrac{\sin t}{t}$ and the value

$$\int_{-\infty}^{\infty} \frac{\sin t}{t}\,dt = \pi \tag{15.2.7}$$

obtained in (12.11.1) lead to the nontrivial integral

$$\int_{-\infty}^{\infty} \frac{\cos x\,\sin\sqrt{x^2+1}}{\sqrt{x^2+1}}\,dx = \frac{\pi}{2}. \tag{15.2.8}$$

The current version of `Mathematica` (the 8th) is unable to evaluate this integral.

15.3. The case of rational integrands

In the special case that the integrand $f(x)$ is a rational function, Theorem 15.2.1 gives an identity among two rational integrals. This is the content of the next theorem.

Theorem 15.3.1. *Assume $f(x)$ is a rational function. Then $\mathfrak{L}(f(x))$ is also rational.*

Proof. If $f(x)$ is a rational function, then

$$f(x+\sqrt{x^2+1})+f(x-\sqrt{x^2+1})$$

and

$$\frac{f(x+\sqrt{x^2+1})-f(x-\sqrt{x^2+1})}{\sqrt{x^2+1}}$$

are also rational functions. Indeed, let $y=\sqrt{x^2+1}$ and assume $f(x)=A(x)/B(x)$. Then

$$\begin{aligned} f(x+y)+f(x-y) &= \frac{A(x+y)}{B(x+y)}+\frac{A(x-y)}{B(x-y)} \\ &= \frac{A(x+y)B(x-y)+A(x-y)B(x+y)}{B(x+y)B(x-y)}. \end{aligned}$$

The numerator is a polynomial in x and y, invariant under $y \mapsto -y$. Therefore it is a polynomial in $y^2=x^2+1$, thus a polynomial in x. The same argument applies to the denominator. □

Example 15.3.2. Let

$$f(x)=\frac{1}{4x^2+12x+21}. \tag{15.3.1}$$

Then

$$\mathfrak{L}(f(x))=\frac{50}{336x^2+408x+481}. \tag{15.3.2}$$

Both integrals may be evaluated in elementary terms to produce the common value

$$\int_{-\infty}^{\infty} f(x)\,dx=\int_{-\infty}^{\infty}\mathfrak{L}(f(x))\,dx=\frac{\pi}{4\sqrt{3}}. \tag{15.3.3}$$

Note 15.3.3. A Landen transformation of a rational function has been defined as a map of the function's coefficients. For instance, applying $\mathfrak{L}$ to the function

$$f(x) = \frac{1}{ax^2 + bx + c} \tag{15.3.4}$$

yields

$$\mathfrak{L}(f(x)) = \frac{1}{a_1x^2 + b_1x + c_1} \tag{15.3.5}$$

with

$$a_1 = \frac{2\,c\,a}{c+a}, \quad b_1 = \frac{b(c-a)}{c+a}, \quad c_1 = \frac{(c+a)^2 - b^2}{2(c+a)}. \tag{15.3.6}$$

Exercise 15.3.4. Check that the discriminant of the denominator is preserved, that is, $b^2 - 4ac = b_1^2 - 4a_1c_1$.

Note 15.3.5. Define

$$\Phi_2(a, b, c) = (a_1, b_1, c_1) \tag{15.3.7}$$

with (a_1, b_1, c_1) given in (15.3.6). Iteration of Φ_2 gives a sequence (a_n, b_n, c_n) that preserves the original integral

$$\int_{-\infty}^{\infty} \frac{dx}{a_nx^2 + b_nx + c_n} = \int_{-\infty}^{\infty} \frac{dx}{ax^2 + bx + c}. \tag{15.3.8}$$

Exercise 15.3.6. Prove that (a_n, b_n, c_n) converges to $(L, 0, L)$, for some $L \in \mathbb{R}$, under the assumption $b^2 - 4ac < 0$.

Passing to the limit in (15.3.8) shows that

$$\int_{-\infty}^{\infty} \frac{dx}{ax^2 + bx + c} = \frac{\pi}{L}. \tag{15.3.9}$$

In the case $a > 0$, the limiting value

$$L = \frac{1}{2}\sqrt{4ac - b^2} \tag{15.3.10}$$

is obtained from (15.3.9) by computing the integral. The case of $a < 0$ is similar.

The map Φ_2 is the rational analog of the classical **arithmetic-geometric mean** presented at the beginning of this chapter. A discussion of this case is presented in Section 15.6.

Exercise 15.3.7. It is possible for a single integral to admit a variety of Landen transformations. For instance the quadratic integral

$$\int_{-\infty}^{\infty} \frac{dx}{ax^2+bx+c} \tag{15.3.11}$$

is also invariant under the change of parameters

$$\begin{aligned} a_{n+1} &= a_n \left[\frac{(a_n+3c_n)^2-3b_n^2}{(3a_n+c_n)(a_n+3c_n)-b_n^2} \right], \\ b_{n+1} &= b_n \left[\frac{3(a_n-c_n)^2-b_n^2}{(3a_n+c_n)(a_n+3c_n)-b_n^2} \right], \\ c_{n+1} &= c_n \left[\frac{(3a_n+c_n)^2-3b_n^2}{(3a_n+c_n)(a_n+3c_n)-b_n^2} \right], \end{aligned} \tag{15.3.12}$$

with $a_0 = a$, $b_0 = b$, and $c_0 = c$. This is described in complete detail in the paper by D. Manna and V. Moll [**208**]. Follow the steps given there to show that iteration of this converges to the stated limit $(L, 0, L)$.

15.4. The evaluation of a quartic integral

This section contains an application of the transformation $\mathfrak{L}$ introduced in Theorem 15.2.1 to the evaluation of the definite integral

$$N_{0,4}(a;m) = \int_0^{\infty} \frac{dx}{(x^4+2ax^2+1)^{m+1}}. \tag{15.4.1}$$

The first theorem describes the effect of $\mathbb{L}$ on the integrand.

Theorem 15.4.1. *For $m \in \mathbb{N}$, let*

$$Q(x) = \frac{1}{(x^4+2ax^2+1)^{m+1}}. \tag{15.4.2}$$

Then

$$Q_1(y) := \mathfrak{L}(Q(x)) = \frac{T_m(2y)}{2^m(1+a+2y^2)^{m+1}}, \tag{15.4.3}$$

where

$$T_m(y) = \sum_{k=0}^{m} \binom{m+k}{m-k} y^{2k}. \tag{15.4.4}$$

Proof. Introduce the variable $\phi = y + \sqrt{y^2+1}$. Then $y - \sqrt{y^2+1} = -\phi^{-1}$ and $2y = \phi - \phi^{-1}$. Moreover,

$$\begin{aligned} Q_1(y) &= \left[Q(\phi) + Q(\phi^{-1})\right] + \frac{\phi^2-1}{\phi^2+1}\left(Q(\phi) - Q(\phi^{-1})\right) \\ &= \frac{2}{\phi^2+1}\left[\phi^2 Q(\phi) + Q(\phi^{-1})\right] \\ &:= S_m(\phi). \end{aligned}$$

Then (15.4.3) is equivalent to

$$2^m\left(1 + a + \tfrac{1}{2}(\phi - \phi^{-1})^2\right)^{m+1} S_m(\phi) = T_m(\phi - \phi^{-1}). \tag{15.4.5}$$

A direct (but lengthy) simplification of the left-hand side of (15.4.5) shows that this identity is equivalent to proving

$$\frac{\phi^{2m+1} + \phi^{-(2m+1)}}{\phi + \phi^{-1}} = T_m(\phi - \phi^{-1}). \tag{15.4.6}$$

Observe that the parameter a has disappeared.

First proof. One simply checks that both sides of (15.4.6) satisfy the second-order recurrence

$$c_{m+2} - (\phi^2 + \phi^{-2})c_{m+1} + c_m = 0 \tag{15.4.7}$$

and that the values for $m = 0$ and $m = 1$ match. This is straightforward for the expression on the left-hand side, while the WZ-method settles the right-hand side. □

Second proof. In the textbook by R. Graham, D. Knuth, and O. Patashnik [**145**], one finds the generating function

$$B_t(z) = \sum_{k \geq 0} (tk)_{k-1} \frac{z^k}{k!}, \tag{15.4.8}$$

where $(a)_k = a(a+1)\cdots(a+k-1)$ is the Pochhammer symbol. The special values

$$B_{-1}(z) = \frac{1 + \sqrt{1+4z}}{2} \quad \text{and} \quad B_2(z) = \frac{1 - \sqrt{1-4z}}{2z} \tag{15.4.9}$$

are combined to produce the identity

$$\frac{1}{\sqrt{1+4z}}\left(B_{-1}(z)^{n+1} - (-z)^{n+1}B_2(-z)^{n+1}\right) = \sum_{k=0}^{n}\binom{n-k}{k} z^k.$$

Replace n by $2m$ and z by $(4y^2)^{-1}$ to produce

$$\frac{1}{2\sqrt{1+y^2}\,(2y)^{2m}}(\phi^{2m+1}+\phi^{-(2m+1)}) = \sum_{k=0}^{m}\binom{2m-k}{k}z^k.$$

The sum on the right-hand side is simplified by the identity

$$T_m(y) = \sum_{k=0}^{m}\binom{m+k}{m-k}y^{2k} = y^{2m}\sum_{k=0}^{m}\binom{2m-k}{k}y^{-2k}.$$

Thus,

$$T_m(\phi-\phi^{-1}) = T_m(2y) = (2y)^{2m}\sum_{k=0}^{m}\binom{2m-k}{k}z^k,$$

and it follows that

$$T_m(\phi-\phi^{-1}) = \frac{1}{2\sqrt{1+y^2}}(\phi^{2m+1}+\phi^{-(2m+1)}),$$

and the result is obtained from $\phi+\phi^{-1} = 2\sqrt{y^2+1}$.

Evaluation of the integral $N_{0,4}(a;m)$. The identity in Theorem 15.2.1 shows that

$$\int_0^\infty Q(x)\,dx = \int_0^\infty Q_1(y)\,dy, \tag{15.4.10}$$

and this last integral can be evaluated in elementary form. Indeed,

$$\begin{aligned}\int_0^\infty Q_1(y)\,dy &= \int_0^\infty \frac{T_m(2y)\,dy}{2^m(1+2y^2)^{m+1}}\\ &= \frac{1}{2^m}\sum_{k=0}^{m}\binom{m+k}{m-k}\int_0^\infty \frac{(2y)^{2k}\,dy}{(1+a+2y^2)^{m+1}}.\end{aligned}$$

The change of variables $y = t\sqrt{1+a}/\sqrt{2}$ gives

$$\int_0^\infty Q_1(y)\,dy = \frac{1}{[2(1+a)]^{m+1/2}}\sum_{k=0}^{m}\binom{m+k}{m-k}2^k(1+a)^k\int_0^\infty \frac{t^{2k}\,dt}{(1+t^2)^{m+1}}.$$

Exercise 15.4.2. Prove the Wallis-type identity

$$\int_0^\infty \frac{t^{2k}\,dt}{(1+t^2)^{m+1}} = \frac{\pi}{2^{2m+1}}\binom{2k}{k}\binom{2m-2k}{m-k}\binom{m}{k}^{-1}. \tag{15.4.11}$$

The previous exercise now produces

$$\int_0^\infty Q_1(y)\,dy = \frac{\pi}{2^{2m+1}}\frac{1}{[2(1+a)]^{m+1/2}} \\ \times \sum_{k=0}^m \binom{m+k}{m-k}2^k\binom{2k}{k}\binom{2m-2k}{m-k}\binom{m}{k}^{-1}(1+a)^k.$$

This can be simplified further using

$$\binom{m+k}{m-k}\binom{2k}{k} = \binom{m+k}{m}\binom{m}{k}, \quad 0 \leq k \leq m, \tag{15.4.12}$$

and (15.4.10) to produce

$$\int_0^\infty Q(y)\,dy = \frac{\pi}{2^{2m+1}}\frac{1}{[2(1+a)]^{m+1/2}}\sum_{k=0}^m 2^k\binom{m+k}{m}\binom{2m-2k}{m-k}(1+a)^k.$$

Theorem 15.4.3. *The integral* $N_{0,4}(a;m)$*, defined in* (15.4.1)*, is given by*

$$N_{0,4}(a;m) = \frac{\pi}{2}\frac{1}{[2(1+a)]^{m+1/2}}\sum_{j=0}^m d_{j,m}a^j, \tag{15.4.13}$$

where

$$d_{j,m} = 2^{-2m}\sum_{k=j}^m 2^k\binom{2m-2k}{m-k}\binom{m+k}{m}\binom{k}{j}. \tag{15.4.14}$$

Note 15.4.4. The literature contains a variety of proofs of the formula given in Theorem 15.4.3. This is written here as

$$N_{0,4}(a;m) = \int_0^\infty \frac{dx}{(x^4+2ax^2+1)^{m+1}} = \frac{\pi}{2}\frac{P_m(a)}{[2(a+1)]^{m+1/2}} \tag{15.4.15}$$

where

$$P_m(a) = \sum_{j=0}^m d_{j,m}a^j. \tag{15.4.16}$$

This note discusses some of these proofs and highlights the remarkable properties of the coefficients $d_{j,m}$.

The first proof. This proof is due to George Boros, a former student of the author. The idea is remarkably simple but has profound consequences. The change of variables $x = \tan\theta$ yields

$$N_{0,4}(a;m) = \int_0^{\pi/2} \left(\frac{\cos^4\theta}{\sin^4\theta + 2a\sin^2\theta\cos^2\theta + \cos^4\theta} \right)^{m+1} \times \frac{d\theta}{\cos^2\theta}.$$

Observe that the denominator of the integrand is a polynomial in $\cos 2\theta$. In terms of the double-angle $u = 2\theta$, the original integral becomes

$$N_{0,4}(a;m) = 2^{-(m+1)} \int_0^{\pi} \left(\frac{(1+\cos u)^2}{(1+a) + (1-a)\cos^2 u} \right)^{m+1} \times \frac{du}{1+\cos u}.$$

Expanding the binomial $(1+\cos u)^{2m+1}$, symmetry implies that

$$\int_0^{\pi} \frac{(\cos u)^j \, du}{[(1+a)+(1-a)\cos^2 u]^{m+1}} = 0,$$

for j odd. The remanining integrals, those with j even, can be evaluated by using the double-angle trick one more time. This leads to

$$N_{0,4}(a;m) = \sum_{j=0}^{m} 2^{-j} \binom{2m+1}{2j} \int_0^{\pi} \frac{(1+\cos v)^j \, dv}{[(3+a)+(1-a)\cos v]^{m+1}},$$

where $v = 2u$ and the symmetry of cosine about $v = \pi$ has been used to reduce the integrals from $[0, 2\pi]$ to $[0, \pi]$. The familiar change of variables $z = \tan(v/2)$ produces the form (15.4.15). The expression obtained for the coefficients $d_{j,m}$ is not very pretty:

$$d_{j,m} = \sum_{r=0}^{j} \sum_{s=0}^{m-j} \sum_{k=j+s}^{m} \frac{(-1)^{k-j-s}}{2^{3k}} \binom{2k}{k} \binom{2m+1}{2s+2r} \binom{m-s-r}{m-k} \times \binom{s+r}{r} \binom{k-s-r}{j-r}.$$

A detour into the world of Ramanujan. The search for a simpler expression for the coefficients $d_{j,m}$ began with the observation that *they appear to be positive.* Indeed, a symbolic calculation shows that for $m = 5$, these are

$$\{d_{j,5} : 0 \leq j \leq 5\} = \left\{ \frac{4389}{256}, \frac{8589}{128}, \frac{7161}{64}, \frac{777}{8}, \frac{693}{16}, \frac{63}{8} \right\}.$$

The second proof of (15.4.15) begins with the value of the elementary integral

$$\int_0^\infty \frac{dx}{bx^4 + 2ax^2 + 1} = \frac{\pi}{2\sqrt{2}} \frac{1}{\sqrt{a + \sqrt{b}}} \tag{15.4.17}$$

and the functions $h(c) = \sqrt{a + \sqrt{1 + c}}$ and

$$g(c) = \int_0^\infty \frac{dx}{x^4 + 2ax^2 + 1 + c}.$$

Then (15.4.17) gives $g'(c) = \pi\sqrt{2}\,h'(c)$. In particular,

$$h'(0) = \frac{1}{\pi\sqrt{2}} N_{0,4}(a; 0).$$

Further differentiation gives the higher-order derivatives of h in terms of the integrals $N_{0,4}$. This is expressed as

Theorem 15.4.5. *The Taylor expansion of* $h(c) = \sqrt{a + \sqrt{1 + c}}$ *is given by*

$$\sqrt{a + \sqrt{1 + c}} = \sqrt{a + 1} + \frac{1}{\pi\sqrt{2}} \sum_{k=1}^\infty \frac{(-1)^{k-1}}{k} N_{0,4}(a; k - 1)c^k.$$

The evaluation of the integrals $N_{0,4}(a; m)$ is now finished by using the **Ramanujan master theorem** stated below.

Theorem 15.4.6. *Suppose* F *has a Taylor expansion around* $c = 0$ *of the form*

$$F(c) = \sum_{k=0}^\infty \frac{(-1)^k}{k!} \varphi(k)\, c^k.$$

Then, the moments of F*, defined by*

$$M_n = \int_0^\infty c^{n-1} F(c)\, dc,$$

can be computed via $M_n = \Gamma(n)\varphi(-n)$.

B. Berndt [**49**], in the first volume of **Ramanujan's Notebooks**, provides a proof of the exact hypothesis for the validity of this theorem. Applications to the evaluation of a large variety of definite integrals are given in the paper by T. Amdeberhan, O. Espinosa, I. Gonzalez, M. Harrison, V. Moll, and A. Straub [**8**]. It turns out that, in the case considered here, the moments can be evaluated explicitly, leading to the proof. Details can be found in the paper by G. Boros and V. Moll [**64**].

A nice short proof. The following argument was communicated to the author by M. Hirschhorn [**171**]. Start with

$$I = \int_0^\infty \frac{dx}{x^4 + 2ax^2 + 1}.$$

Make the substitution $x \mapsto 1/x$ and add the two forms of the integral I to obtain

$$2I = \int_0^\infty \frac{(x^2+1)\,dx}{x^4 + 2ax^2 + 1}.$$

The second substitution $y = x - 1/x$ gives

$$2I = \int_{-\infty}^\infty \frac{dy}{y^2 + 2a + 2} = \frac{\pi}{\sqrt{2a+2}}.$$

Now, for an appropriate value of c (to guarantee convergence),

$$\int_0^\infty \frac{dx}{x^4 + 2ax^2 + c^2} = \frac{\pi}{2\sqrt{2}\,\sqrt{a+c}}.$$

Differentiation with respect to c leads to the identity

$$\int_0^\infty \frac{dx}{(x^4 + 2ax^2 + c^2)^{m+1}} = \frac{\pi}{2^{3m+3/2}\,c^{2m+1}\,(a+c)^{m+1/2}} \times \sum_{k=0}^{m} 2^{m-k} \binom{2k}{k} \binom{2m-k}{m} c^k (a+c)^{m-k}.$$

The result now follows by taking $c = 1$.

Proofs in other styles. There are several other proofs of Theorem 15.4.3 in the literature. The paper by G. Boros and V. Moll [**62**] produced a proof based on elementary properties of the hypergeometric function plus an entry from the table by I. S. Gradshteyn and I. M. Ryzhik [**144**]. A new proof based on a method for the evaluation of integrals coming from Feynman diagrams appears in the paper by T. Amdeberhan, V. Moll, and C. Vignat [**15**]. An automatic proof has appeared in the work of C. Koutschan and V. Levandovskyy [**187**] and one more based on the study of statistical densities can be found in the work by C. Berg and C. Vignat [**48**]. Finally, a nice evaluation combining classical and automatic methods appears in the paper by

M. Apagodu [**23**]. **The reader is encouraged to produce his/her own**.

The coefficients $d_{j,m}$. These numbers have remarkable properties.

A related family of polynomials. Start with

$$P_m(a) = \frac{2}{\pi}\,[2(a+1)]^{m+\frac{1}{2}} \int_0^\infty \frac{dx}{(x^4+2ax^2+1)^{m+1}},$$

and compute $d_{j,m}$ as coming from the Taylor expansion at $a=0$ of the right-hand side. This yields

(15.4.18)
$$d_{j,m} = \frac{1}{j!m!2^{m+j}}\left(\alpha_j(m)\prod_{k=1}^{m}(4k-1) - \beta_j(m)\prod_{k=1}^{m}(4k+1)\right),$$

where α_j and β_j are polynomials in m of degrees j and $j-1$, respectively. The explicit expressions

$$\alpha_j(m) = \sum_{t=0}^{\lfloor j/2\rfloor}\binom{j}{2t}\prod_{\nu=m+1}^{m+t}(4\nu-1)\prod_{\nu=m-j+2t+1}^{m}(2\nu+1)\prod_{\nu=1}^{t-1}(4\nu+1)$$

and

$$\beta_j(m) = \sum_{t=1}^{\lfloor (j+1)/2\rfloor}\binom{j}{2t-1}\prod_{\nu=m+1}^{m+t-1}(4\nu{+}1)\prod_{\nu=m-j+2t}^{m}(2\nu{+}1)\prod_{\nu=1}^{t-1}(4\nu{-}1)$$

are given in the paper by G. Boros, V. Moll, and J. Shallit [**67**].

Trying to obtain more information about the polynomials α_j and β_j directly proved difficult. One uninspired day, the author decided to compute their roots numerically. It was a pleasant surprise to discover the following property.

Theorem 15.4.7. *For all $j \geq 1$, all the roots of $\alpha_j(m)=0$ lie on the line* $\text{Re}\, m = -\frac{1}{2}$. *Similarly, the roots of $\beta_j(m)=0$ for $j \geq 2$ lie on the same vertical line.*

The proof of this theorem, due to J. Little [**201**], starts by writing

(15.4.19) $\quad A_j(s) := \alpha_j((s-1)/2) \quad$ and $\quad B_j(s) := \beta_j((s-1)/2)$

and proving that A_j is equal to $j!$ times the coefficient of u^j in $f(s,u)g(s,u)$, where $f(s,u) = (1+2u)^{s/2}$ and $g(s,u)$ is the hypergeometric series

$$g(s,u) = {}_2F_1\left(\frac{s}{2}+\frac{1}{4}, \frac{1}{4}; \frac{1}{2}; 4u^2\right). \tag{15.4.20}$$

A similar expression is obtained for $B_j(s)$. From here it follows that A_j and B_j each satisfy the three-term recurrence

$$x_{j+1}(s) = 2sx_j(s) - (s^2-(2j-1)^2)x_{j-1}(s). \tag{15.4.21}$$

Little then establishes a version of Sturm's theorem about interlacing zeros to prove the final result.

The location of the zeros of $\alpha_j(m)$ now suggests studying the behavior of this family as $j \to \infty$. In the best of all worlds, one will obtain an analytic function of m with all the zeros on a vertical line. Perhaps some number theory will enter and ... *one never knows*.

Arithmetical properties. The expression (15.4.18) gives

$$m!2^{m+1}\, d_{1,m} = (2m+1)\prod_{k=1}^{m}(4k-1) - \prod_{k=1}^{m}(4k+1), \tag{15.4.22}$$

from which it follows that the right-hand side is an even number. This led naturally to the problem of determining the 2-adic valuation of

$$\begin{aligned} A_{j,m} := j!m!2^{m+j}d_{j,m} &= \alpha_j(m)\prod_{k=1}^{m}(4k-1) - \beta_j(m)\prod_{k=1}^{m}(4k+1) \\ &= \frac{j!m!}{2^{m-j}}\sum_{k=j}^{m} 2^k\binom{2m-2k}{m-k}\binom{m+k}{k}\binom{k}{j}. \end{aligned}$$

The main result of [**67**] is that $\nu_2(A_{j,m}) = \nu_2(m(m+1))+1$. This was extended in the work of T. Amdeberhan, D. Manna, and V. Moll [**9**] to the next theorem.

Theorem 15.4.8. *The 2-adic valuation of $A_{j,m}$ satisfies*

$$\nu_2(A_{j,m}) = \nu_2((m+1-j)_{2j}) + j, \tag{15.4.23}$$

where $(a)_k = a(a+1)\cdots(a+k-1)$ is the Pochhammer symbol for $k \geq 1$, with $(a)_0 = 1$.

The proof is an elementary application of the WZ-method. Define the numbers

$$B_{j,m} := \frac{A_{j,m}}{2^j(m+1-j)_{2j}},$$

and use the WZ-method to obtain the recurrence

$$B_{j-1,m} = (2m+1)B_{j,m} - (m-j)(m+j+1)B_{j+1,m}, \quad 1 \leq j \leq m-1.$$

Since the initial values $B_{m,m} = 1$ and $B_{m-1,m} = 2m+1$ are odd, it follows inductively that $B_{j,m}$ is an odd integer. The reader will also find in [**9**] a WZ-free proof of the theorem.

The combinatorics of the valuations. The sequence of valuations $\{\nu_2(A_{j,m}) : m \geq j\}$ increases in complexity with j. Some of the combinatorial nature of this sequence is described next. The first feature of this sequence is that it has a block structure, reminiscent of the simple functions of real analysis.

Definition 15.4.9. Let $s \in \mathbb{N}$, $s \geq 2$. The sequence $\{a_j : j \in \mathbb{N}\}$ has **block structure** if there is an $s \in \mathbb{N}$ such that for each $t \in \{0, 1, 2, \ldots\}$,

$$a_{st+1} = a_{st+2} = \cdots = a_{s(t+1)}. \tag{15.4.24}$$

The sequence is called s**-simple** if s is the largest value for which (15.4.24) occurs.

Theorem 15.4.10. *For each $j \geq 1$, the set*

$$X(j) := \{\nu_2(A_{j,m}) : m \geq j\}$$

is an s-simple sequence, with $s = 2^{1+\nu_2(j)}$.

Valuation patterns encoded in binary trees. The goal is to describe precisely the graph of the sequence $\{\nu_2(A_{j,m}) : m \geq j\}$. The reader is referred to the paper by X. Sun and V. Moll [**287**] for complete details. In view of the block structure described earlier, it suffices to consider the sequences $\{\nu_2(C_{j,m}) : m \geq j\}$, which are defined by

$$C_{j,m} = A_{j,j+(m-1)\cdot 2^{1+\nu_2(j)}},$$

so that the sequence $\{C_{j,m} : m \geq j\}$ reduces each block of $A_{j,m}$ to a single point. The emerging patterns are still very complicated. For instance, Figure 15.4.1 shows the case of $j = 13$ and $j = 59$. The remarkable fact is that in spite of the complexity of $\nu_2(C_{j,m})$ there is **an exact formula** for it. We now describe how to find it.

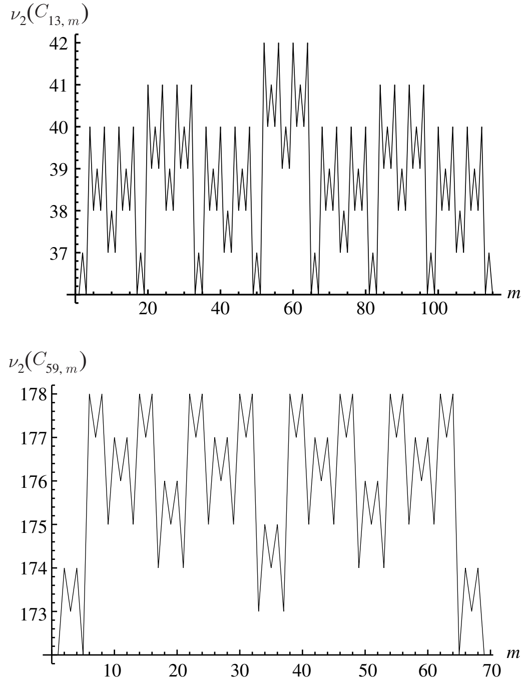


Figure 15.4.1. The valuations $\nu_2(C_{13,m})$ and $\nu_2(C_{59,m})$.

The construction of the **decision tree** associated to the index j starts with a root v_0 at level $k = 0$. To this vertex attach the sequence $\{\nu_2(C_{j,m}) : m \geq 1\}$ and ask whether $\nu_2(C_{j,m}) - \nu_2(m)$ has a constant value *independent* of m. If the answer is yes, then it is said that v_0 is a **terminal vertex** and we label it with this constant. The tree is complete. If the answer is negative, split the integers modulo 2 and produce two new vertices, v_1, v_2, connected to v_0 and attach the classes $\{\nu_2(C_{j,2m-1}) : m \geq 1\}$ and $\{\nu_2(C_{j,2m}) : m \geq 1\}$ to these vertices. Now ask whether $\nu_2(C_{j,2m-1}) - \nu_2(m)$ is independent of m and the same for $\nu_2(C_{j,2m}) - \nu_2(m)$. Each vertex that yields a positive answer is considered terminal and the corresponding constant value is attached to it. Every vertex with a negative answer produces two new ones at the next level.

Assume that the vertex v corresponding to the sequence $\{2^k(m-1)+a : m \geq 1\}$ produces a negative answer. Then it splits in the next generation into two vertices corresponding to the sequences $\{2^{k+1}(m-1)+a : m \geq 1\}$ and $\{2^{k+1}(m-1)+2^k+a : m \geq 1\}$. For instance, in Figure 15.4.2, the vertex corresponding to $\{4m : m \geq 1\}$, which is not terminal, splits into $\{8m : m \geq 1\}$ and $\{8m-4 : m \geq 1\}$. These two edges lead to terminal vertices. Theorem 15.4.11 shows that this process ends in a finite number of steps.

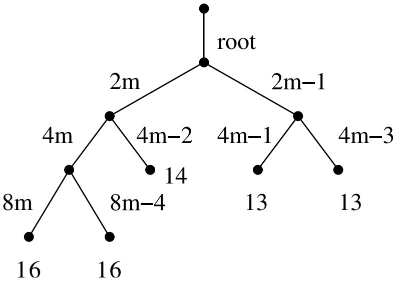


Figure 15.4.2. The decision tree for $j = 5$.

Theorem 15.4.11. *Let $j \in \mathbb{N}$ and let $T(j)$ be its decision tree. Define $k^*(j) := \lfloor \log_2 j \rfloor$. Then* (1) *$T(j)$ depends only on the odd part of j; that is, if $r \in \mathbb{N}$, then $T(j) = T(2^r j)$, up to the labels.* (2) *The generations of the tree are labelled starting at* 0*; that is, the root is generation* 0*. Then, for $0 \leq k \leq k^*(j)$, the kth generation of $T(j)$ has 2^k vertices. Up to that point, $T(j)$ is a complete binary tree.* (3) *The k^*th generation contains $2^{k^*+1} - j$ terminal vertices. The constants associated with these vertices are given by the following algorithm. Define $j_1(j,k,a) := -j + 2(1 + 2^k - a)$ and*

$$\gamma_1(j,k,a) = j + k + 1 + \nu_2\left((j_1 + j - 1)!\right) + \nu_2\left((j - j_1)!\right).$$

Then, for $1 \leq a \leq 2^{k^*+1} - j$,

$$\nu_2\left(C_{j,2^k(m-1)+a}\right) = \nu_2(m) + \gamma_1(j,k,a).$$

Thus, the vertices at the k^**th generation have constants given by* $\gamma_1(j,k,a)$. (4) *The remaining terminal vertices of the tree* $T(j)$ *appear in the next generation. There are* $2(j-2^{k^*(j)})$ *of them. The constants attached to these vertices are defined as follows: let*

$$j_2(j,k,a) := -j+2(1+2^{k+1}-a) \quad \textit{and} \quad j_3(j,k,a) := j_2(j,k,a+2^k).$$

Define

$$\gamma_2(j,k,a) := j+k+2+\nu_2\left((j_2+j-1)!\right)+\nu_2\left((j-j_2)!\right)$$

and

$$\gamma_3(j,k,a) := j+k+2+\nu_2\left((j_3+j-1)!\right)+\nu_2\left((j-j_3)!\right).$$

Then, for $2^{k^*(j)+1}-j+1 \leq a \leq 2^{k^*(j)}$,

$$\nu_2\left(C_{j,2^{k^*(j)+1}(m-1)+a}\right) = \nu_2(m)+\gamma_2(j,k^*(j),a)$$

and

$$\nu_2\left(C_{j,2^{k^*(j)+1}(m-1)+a+2^{k^*(j)}}\right) = \nu_2(m)+\gamma_3(j,k^*(j),a)$$

give the constants attached to these remaining terminal vertices.

The theorem is now employed to produce an analytic formula for $\nu_2(C_{3,m})$. The value $k^*(3)=1$ shows that the first level contains $2^{1+1}-3=1$ terminal vertex. This corresponds to the sequence $2m-1$ and has constant value 7. Thus,

$$\nu_2\left(C_{3,2m-1}\right) = 7. \tag{15.4.25}$$

The next level has $2(3-2^1)=2$ terminal vertices. These correspond to the sequences $4m$ and $4m-2$, with constant value 9 for both of them. This tree produces

$$\nu_2\left(C_{3,m}\right) = \begin{cases} 7+\nu_2\left(\frac{m+1}{2}\right) & \text{if } m \equiv 1 \bmod 2, \\ 9+\nu_2\left(\frac{m}{4}\right) & \text{if } m \equiv 0 \bmod 4, \\ 9+\nu_2\left(\frac{m+2}{4}\right) & \text{if } m \equiv 2 \bmod 4. \end{cases} \tag{15.4.26}$$

The complexity of the graph for $j = 13$ is reflected in the analytic formula for this valuation. The theorem yields

$$\nu_2\left(C_{13,m}\right) = \begin{cases} 36 + \nu_2\left(\frac{m+7}{8}\right) & \text{if } m \equiv 1 \bmod 8, \\ 37 + \nu_2\left(\frac{m+6}{8}\right) & \text{if } m \equiv 2 \bmod 8, \\ 36 + \nu_2\left(\frac{m+5}{8}\right) & \text{if } m \equiv 3 \bmod 8, \\ 40 + \nu_2\left(\frac{m+12}{16}\right) & \text{if } m \equiv 4 \bmod 16, \\ 38 + \nu_2\left(\frac{m+11}{16}\right) & \text{if } m \equiv 5 \bmod 16, \\ 39 + \nu_2\left(\frac{m+10}{16}\right) & \text{if } m \equiv 6 \bmod 16, \\ 38 + \nu_2\left(\frac{m+9}{16}\right) & \text{if } m \equiv 7 \bmod 16, \\ 40 + \nu_2\left(\frac{m+8}{16}\right) & \text{if } m \equiv 8 \bmod 16, \\ 40 + \nu_2\left(\frac{m+4}{16}\right) & \text{if } m \equiv 12 \bmod 16, \\ 38 + \nu_2\left(\frac{m+3}{16}\right) & \text{if } m \equiv 13 \bmod 16, \\ 39 + \nu_2\left(\frac{m+2}{16}\right) & \text{if } m \equiv 14 \bmod 16, \\ 38 + \nu_2\left(\frac{m+1}{16}\right) & \text{if } m \equiv 15 \bmod 16, \\ 40 + \nu_2\left(\frac{m}{16}\right) & \text{if } m \equiv 16 \bmod 16. \end{cases} \tag{15.4.27}$$

Note. The p-adic valuations of $A_{j,m}$ for p odd have different behavior from the case $p = 2$. Figure 15.4.3 shows the plot of $\nu_{17}(A_{1,m})$ where linear growth is observed. Experimental data suggest that, for any odd prime p, one has

$$\nu_p(A_{j,m}) \sim \frac{m}{p-1}. \tag{15.4.28}$$

The error term $\nu_{17}(A_{1,m}) - m/16$ is also shown in the figure. The structure of the error remains to be explored.

Unimodality and logconcavity. A finite sequence of real numbers $\{a_0, a_1, \ldots, a_m\}$ is said to be **unimodal** if there exists an index $0 \leq j \leq m$ such that $a_0 \leq a_1 \leq \cdots \leq a_j$ and $a_j \geq a_{j+1} \geq \cdots \geq a_m$. A polynomial is said to be unimodal if its sequence of coefficients is unimodal. The sequence $\{a_0, a_1, \ldots, a_m\}$ with $a_j \geq 0$ is said to be **logarithmically concave** (or **logconcave** for short) if $a_{j+1}a_{j-1} \leq a_j^2$ for $1 \leq j \leq m-1$. A polynomial is said to be logconcave if its sequence of coefficients is logconcave. It is easy to see that if a sequence is logconcave, then it is unimodal. See the book by H. S. Wilf [**313**] for an introduction to these ideas.

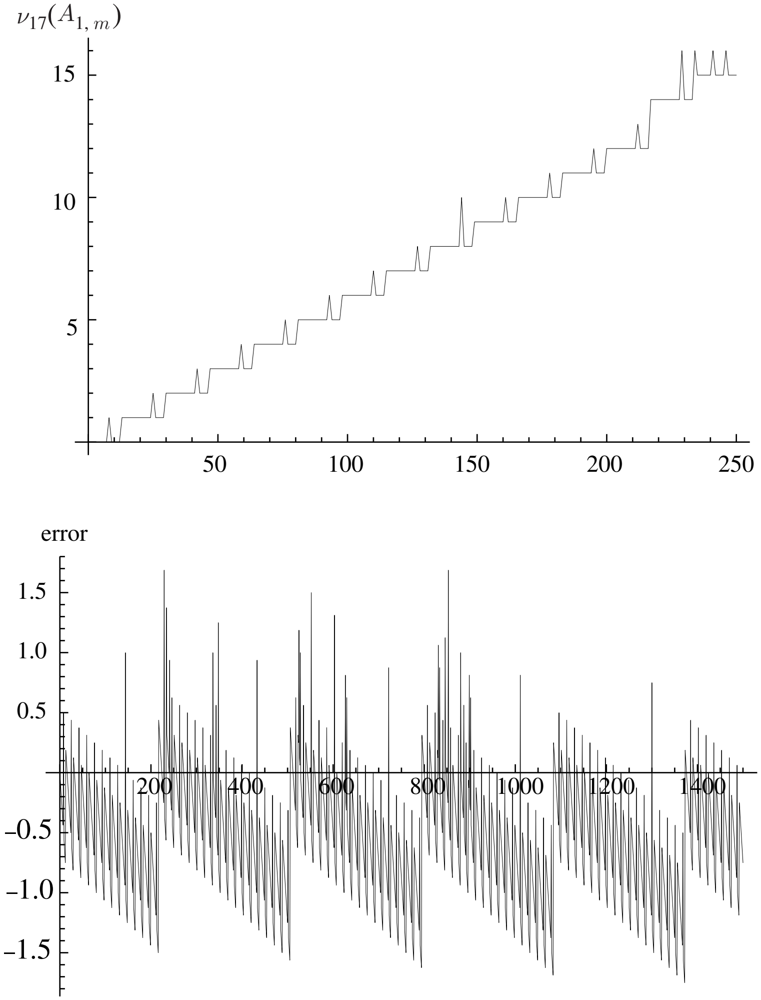


Figure 15.4.3. The valuation $\nu_{17}(A_{1,m})$ and the error term.

Unimodal polynomials arise often in combinatorics, geometry, and algebra and have been the subject of considerable research in recent years. The reader is referred to the papers by F. Brenti [**77**] and R. Stanley [**278**] for surveys of the diverse techniques employed to prove that specific families of polynomials are unimodal.

For $m \in \mathbb{N}$, the sequence $\{d_{j,m} : 0 \leq j \leq m\}$ is unimodal. This is a consequence of the following criterion established in the paper by G. Boros and V. Moll [**61**].

Theorem 15.4.12. *Let a_k be a nondecreasing sequence of positive numbers and let $A(x) = \sum_{k=0}^{m} a_k x^k$. Then $A(x+1)$ is unimodal.*

This theorem was applied to the polynomial

$$A(x) := 2^{-2m} \sum_{k=0}^{m} 2^k \binom{2m-2k}{m-k} \binom{m+k}{m} x^k \tag{15.4.29}$$

that satisfies $P_m(x) = A(x+1)$. The criterion was extended in a project at SIMU (Summer Institute in Mathematics for Undergraduates), an REU program in Puerto Rico. The result was the paper by J. Alvarez, M. Amadis, G. Boros, D. Karp, V. Moll, and L. Rosales [**7**] to include the shifts $A(x+j)$ and the paper by Yi Yang and Yeong-Nan Yeh [**304**] for arbitrary shifts. The original proof of the unimodality of $P_m(a)$ can be found in the paper by G. Boros and V. Moll [**63**].

The author conjectured in [**221**] the logconcavity of $\{d_{j,m} : 0 \leq j \leq m\}$. This turned out to be a more difficult question. Some of our failed attempts are described next.

(1) A result of F. Brenti [**77**] states that if $A(x)$ is logconcave, then so is $A(x+1)$. Unfortunately this does not apply in this case since (15.4.29) is not logconcave. Indeed,

$$\begin{aligned} 2^{4m-2k}\left(a_k^2 - a_{k-1}a_{k+1}\right) &= \binom{2m}{m-k}^2 \binom{m+k}{m}^2 \\ &\times \left(1 - \frac{k(m-k)(2m-2k+1)(m+k+1)}{(k+1)(m+k)(2m-2k-1)(m-k+1)}\right) \end{aligned}$$

and this last factor could be negative—for example, for $m = 5$ and $j = 4$. The number of negative terms in this sequence is small, so perhaps there is a way out of this.

(2) The coefficients $d_{j,m}$ satisfy many recurrences. For example,

$$d_{j+1,m} = \frac{2m+1}{j+1} d_{j,m} - \frac{(m+j)(m+1-j)}{j(j+1)} d_{j-1,m}.$$

This can be found by a direct application of the WZ-method. Therefore, $d_{j,m}$ is logconcave provided

$$j(2m+1)d_{j-1,m}d_{j,m} \leq (m+j)(m+1-j)d_{j-1,m}^2 + j(j+1)d_{j,m}^2.$$

The author conjectured that the smallest value of the expression

$$(m+j)(m+1-j)d_{j-1,m}^2 + j(j+1)d_{j,m}^2 - j(2m+1)d_{j-1,m}d_{j,m}$$

is $2^{2m}m(m+1)\binom{2m}{m}^2$ and it occurs at $j = m$. This has been established by W. Y. C. Chen and E. X. W. Yia [**99**]. It implies the logconcavity of $\{d_{j,m} : 0 \leq j \leq m\}$.

Actually, the author has conjectured that the $d_{j,m}$ satisfy a stronger version of logconcavity. Given a sequence $\{a_j\}$ of positive numbers, define a map

$$\mathbb{L}(\{a_j\}) := \{b_j\}$$

by $b_j := a_j^2 - a_{j-1}a_{j+1}$. Thus $\{a_j\}$ is logconcave if $\{b_j\}$ has positive coefficients. The nonnegative sequence $\{a_j\}$ is called **infinitely logconcave** if any number of applications of $\mathbb{L}$ produces a nonnegative sequence.

Conjecture 15.4.13. *For each fixed $m \in \mathbb{N}$, the sequence $\{d_{j,m} : 0 \leq j \leq m\}$ is infinitely logconcave.*

The logconcavity of $\{d_{j,m} : 0 \leq j \leq m\}$ has recently been established by M. Kauers and P. Paule [**180**] as an applications of their work on establishing inequalities by automatic means. The starting point is the triple sum expression for $d_{j,m}$ written as

$$d_{j,m} = \sum_{j,s,k} \frac{(-1)^{k+j-l}}{2^{3(k+s)}} \binom{2m+1}{2s}\binom{m-s}{k}\binom{2(k+s)}{k+s}\binom{s}{j}\binom{k}{l-j}.$$

Using the RISC (Research Institute for Symbolic Computation) package Multisim developed by K. Wegschaider [**308**], Kauers and Paule derived the recurrence

$$2(m+1)d_{j,m+1} = 2(j+m)d_{j-1,m} + (2j+4m+3)d_{j,m}.$$

The positivity of $d_{j,m}$ follows directly from this. To establish the logconcavity of $d_{j,m}$, the new recurrence

$$\begin{aligned}4j(j+1)d_{j+1,m} = {} & -2(2j-4m-3)(j+m+1)d_{j,m} \\ & + 4(j-m-1)(m+1)d_{j,m+1}\end{aligned}$$

is derived automatically and the logconcavity of $d_{j,m}$ is reduced to establishing the inequality

$$d_{j,m}^2 \geq \frac{4(m+1)\left(4(j-m-1)(m+1)-(2j^2-4m^2-7m-3)d_{j,m+1}d_{j,m}\right)}{16m^3+16jm^2+40m^2+28jm+33m+9j+9}.$$

This is now accomplished in automatic fashion.

The 2-logconcavity of $\{d_{j,m} : 0 \leq j \leq m\}$ is not achievable by these methods. At the end of [**180**], M. Kauers and P. Paule state that "...we have little hope that a proof of 2-logconcavity could be completed along these lines, not to mention that a human reader would have a hard time digesting it." Actually, 2-logconcavity has been established by W. Y. C. Chen and E. X. W. Xia in [**98**].

The general concept of infinite logconcavity has generated some interest. D. Uminsky and K. Yeats [**295**] have studied the action of $\mathbb{L}$ on sequences of the form

$$\{\ldots,0,0,1,x_0,x_1,\ldots,x_n,\ldots,x_1,x_0,1,0,0,\ldots\} \tag{15.4.30}$$

and

$$\{\ldots,0,0,1,x_0,x_1,\ldots,x_n,x_n,\ldots,x_1,x_0,1,0,0,\ldots\} \tag{15.4.31}$$

and have established the existence of a large unbounded region in the positive orthant of $\mathbb{R}^n$ that consists only of infinitely logconcave sequences $\{x_0,\ldots,x_n\}$. P. R. McNamara and B. Sagan [**214**] have considered sequences satisfying the condition $a_k^2 \geq ra_{k-1}a_{k+1}$. Clearly this implies logconcavity if $r \geq 1$. Their techniques apply to the rows of the Pascal triangle. Choosing appropriate r-factors and a computer verification procedure, they obtain the following.

Theorem 15.4.14. *The sequence $\{\binom{n}{k} : 0 \leq k \leq n\}$ is infinitely logconcave for fixed $n \leq 1450$.*

Newton began the study of logconcave sequences by establishing the following result (paraphrased in Section 2.2 of the book by G. H. Hardy, J. E. Littlewood, and G. Polya [**159**]).

Theorem 15.4.15. *Let $\{a_k\}$ be a finite sequence of positive real numbers. Assume all the roots of the polynomial*

$$P[a_k; x] := a_0 + a_1 x + \cdots + a_n x^n \tag{15.4.32}$$

are real. Then the sequence $\{a_k\}$ is logconcave.

P. R. McNamara and B. Sagan [**214**] and, independently, R. Stanley (personal communication) and S. Fisk [**129**] have proposed the next problem. This was settled by P. Brändèn [**76**]. See [**214**] for the complete details on the conjecture.

Theorem 15.4.16. *Let $\{a_k\}$ be a finite sequence of positive real numbers. If $P[a_k; x]$ has only real roots, then the same is true for $P[\mathbb{L}(a_k); x]$.*

The polynomials $P_m(a)$ are the generating function for the sequence $\{d_{j,m}\}$ described here. It is an unfortunate fact that they do not have real roots, as established by G. Boros and V. Moll [**63**]. Thus, the previous theorem does not apply to Conjecture 15.4.13. In spite of this, the asymptotic behavior of these zeros has remarkable properties. D. Dimitrov [**111**] has shown that, in the right scale, the zeros converge to a lemniscate.

The infinite logconcavity of $\{d_{j,m}\}$ has resisted all our efforts. It remains to be established.

15.5. An integrand of degree six

The result of Theorem 15.2.1 is now applied to an integral where the integrand is an even rational function of degree six. The result is given in the next theorem.

Theorem 15.5.1. *Define*

$$I(\mathbf{a}, \mathbf{b}) = \int_0^\infty \frac{a_4 x^4 + a_2 x^2 + a_0}{b_6 x^6 + b_4 x^4 + b_2 x^2 + b_0}\, dx.$$

Then

$$I(\mathbf{a},\mathbf{b}) = I(\mathbf{a}^*,\mathbf{b}^*),$$

where

$$\begin{aligned} a_4^* &= 32(a_4b_0 + a_0b_6), \\ a_2^* &= 8(a_2b_0 + 3a_4b_0 + a_4b_2 + a_0b_4 + 3a_0b_6 + a_2b_6), \\ a_0^* &= 2(a_0 + a_2 + a_4)(b_0 + b_2 + b_4 + b_6) \end{aligned}$$

and

$$\begin{aligned} b_6^* &= 64b_0b_6, \\ b_4^* &= 16(b_0b_4 + 6b_0b_6 + b_2b_6), \\ b_2^* &= 4(b_0b_2 + 4b_0b_4 + b_2b_4 + 9b_0b_6 + 4b_2b_6 + b_4b_6), \\ b_0^* &= (b_0 + b_2 + b_4 + b_6)^2. \end{aligned}$$

The next exercise suggests a scaling that reduces the number of parameters in the problem.

Exercise 15.5.2. Prove that the integral

$$U_6(a,b;c,d,e) := \int_0^\infty \frac{cx^4 + dx^2 + e}{x^6 + ax^4 + bx^2 + 1}\,dx \tag{15.5.1}$$

is invariant under the transformation

$$\begin{aligned} a_{n+1} &= \frac{a_nb_n + 5a_n + 5b_n + 9}{(a_n + b_n + 2)^{4/3}}, \\ b_{n+1} &= \frac{a_n + b_n + 6}{(a_n + b_n + 2)^{2/3}}, \\ c_{n+1} &= \frac{c_n + d_n + e_n}{(a_n + b_n + 2)^{2/3}}, \\ d_{n+1} &= \frac{(b_n + 3)c_n + 2d_n + (a_n + 3)e_n}{a_n + b_n + 2}, \\ e_{n+1} &= \frac{c_n + e_n}{(a_n + b_n + 2)^{1/3}}. \end{aligned} \tag{15.5.2}$$

The first two equations in (15.5.2) are independent of the variables c, d, and e so they define a map

$$\Phi_6(a,b) = \left(\frac{ab + 5a + 5b + 9}{(a + b + 2)^{4/3}}, \frac{a + b + 6}{(a + b + 2)^{2/3}} \right) \tag{15.5.3}$$

that is well-defined on $\mathbb{R}^2$ minus the line $a+b+2=0$. The main result of M. Chamberland and V. Moll [**95**] is stated below.

Theorem 15.5.3. *The set of points in $\mathbb{R}^2$ that converge to the fixed point $(3,3)$ of the dynamical system*

$$\begin{aligned} a_{n+1} &= \frac{a_nb_n+5a_n+5b_n+9}{(a_n+b_n+2)^{4/3}}, \\ b_{n+1} &= \frac{a_n+b_n+6}{(a_n+b_n+2)^{2/3}} \end{aligned} \tag{15.5.4}$$

is the region Λ of the (a,b)-plane for which the integral (15.5.1) *converges.*

Note 15.5.4. The region Λ is given in terms of the **resolvent curve** $\mathfrak{R}$ defined by

$$R(a,b) := 4a^3+4b^3-18ab-a^2b^2+27=0. \tag{15.5.5}$$

This function appeared in Theorem 4.7.12. The set $R(a,b)=0$ is a real algebraic curve with two connected components $\mathfrak{R}_{\pm}$. The component $\mathfrak{R}_+$ is contained in the first quadrant and contains the point $(3,3)$ as a cusp. The second component $\mathfrak{R}_-$ is disjoint from the first quadrant. The region Λ is defined as the points on the ab-plane that are above the curve $\mathfrak{R}_-$.

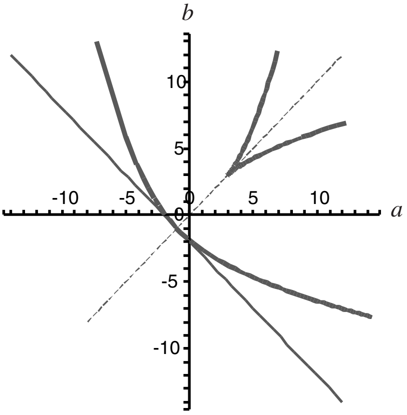


Figure 15.5.1. The resolvent curve.

The identity

$$R(a_1, b_1) \quad = \quad \frac{(a-b)^2 R(a,b)}{(a+b+2)^4} \tag{15.5.6}$$

plays an important role in the dynamics of (15.5.4). In particular it follows from (15.5.6) that the resolvent curve $R(a,b) = 0$, and the regions $\{(a,b) : R(a,b) > 0\}$, located between the two branches in Figure 15.5.1, and $\{(a,b) : R(a,b) < 0\}$ are preserved by Φ_6. The identity (15.5.6) also shows that the diagonal $\Delta = \{(a,b) : a = b\}$ of $\mathbb{R}^2$ is mapped onto the resolvent curve $\mathfrak{R}$. This yields the parametrization

$$a(t) = \frac{t+9}{2^{4/3}(t+1)^{1/3}} \quad \text{and} \quad b(t) = \frac{2^{1/3}(t+3)}{(t+1)^{2/3}}$$

of this curve. This parametrization may be employed to analyze the behavior on the resolvent curve.

Note 15.5.5. The relation between the resolvent curve and the discriminant of a cubic polynomial is clarified in Exercise 4.7.10.

15.6. The original elliptic case

Among the many beautiful results in the theory of elliptic integrals, a calculation of Gauss stands among the best: take two positive real numbers a and b, with $a > b$, and form a new pair by replacing a with the arithmetic mean $(a+b)/2$ and b with the geometric mean $\sqrt{ab}$. Then iterate:

$$a_{n+1} = \frac{a_n + b_n}{2}, \quad b_{n+1} = \sqrt{a_n b_n} \tag{15.6.1}$$

starting with $a_0 = a$ and $b_0 = b$. K. F. Gauss [**133**] was interested in the initial conditions $a = 1$ and $b = \sqrt{2}$. The iteration generates a sequence of algebraic numbers which rapidly become impossible to describe explicitly; for instance,

$$a_3 = \frac{1}{2^3}\left((1 + \sqrt[4]{2})^2 + 2\sqrt{2}\sqrt[8]{2}\sqrt{1+\sqrt{2}} \right) \tag{15.6.2}$$

is a root of the polynomial

$$\begin{aligned} G(a) \quad = \quad & 16777216a^8 - 16777216a^7 + 5242880a^6 - 10747904a^5 \\ & +942080a^4 - 1896448a^3 + 4436a^2 - 59840a + 1. \end{aligned}$$

The numerical behavior is surprising; a_6 and b_6 agree to 87 digits. It is simple to check that

$$\lim_{n \to \infty} a_n = \lim_{n \to \infty} b_n. \tag{15.6.3}$$

This common limit is called the **arithmetic-geometric mean** and is denoted by $\mathrm{AGM}(a, b)$. It is the explicit dependence on the initial condition that is hard to discover.

Gauss computed some numerical values and observed that

$$a_{11} \sim b_{11} \sim 1.198140235 \tag{15.6.4}$$

and then he *recognized* the reciprocal of this number as a numerical approximation to the elliptic integral

$$I = \frac{2}{\pi} \int_0^1 \frac{dt}{\sqrt{1 - t^4}}. \tag{15.6.5}$$

It is unclear to the authors how Gauss recognized this number—he simply knew it. (Stirling's tables may have been a help; the book by J. M. Borwein and D. H. Bailey [**69**] contains a reproduction of the original notes and comments.) He was particularly interested in the evaluation of this definite integral as it provides the length of a lemniscate. In his diary Gauss remarked, *"This will surely open up a whole new field of analysis."* More details can be found in the book by J. M. Borwein and P. B. Borwein [**71**] and the paper by D. Cox [**105**].

Gauss' procedure to find an analytic expression for $\mathrm{AGM}(a, b)$ began with the elementary observation

$$\mathrm{AGM}(a, b) = \mathrm{AGM}\left(\frac{a + b}{2}, \sqrt{ab} \right) \tag{15.6.6}$$

and the homegeneity condition

$$\mathrm{AGM}(\lambda a, \lambda b) = \lambda \mathrm{AGM}(a, b). \tag{15.6.7}$$

He used (15.6.6) with $a = (1+\sqrt{k})^2$ and $b = (1-\sqrt{k})^2$, with $0 < k < 1$, to produce

$$\mathrm{AGM}(1 + k + 2\sqrt{k}, 1 + k - 2\sqrt{k}) = \mathrm{AGM}(1 + k, 1 - k).$$

He then used the homogeneity of AGM to write

$$\begin{aligned}&\mathrm{AGM}(1+k+2\sqrt{k}, 1+k-2\sqrt{k})\\&\qquad=\mathrm{AGM}((1+k)(1+k^*), (1+k)(1-k^*))\\&\qquad=(1+k)\mathrm{AGM}(1+k^*, 1-k^*),\end{aligned}$$

with

(15.6.8) $$k^* = \frac{2\sqrt{k}}{1+k}.$$

This resulted in the functional equation

(15.6.9) $$\mathrm{AGM}(1+k, 1-k) = (1+k)\,\mathrm{AGM}(1+k^*, 1-k^*).$$

In his analysis of (15.6.9), Gauss substituted the power series

(15.6.10) $$\frac{1}{\mathrm{AGM}(1+k, 1-k)} = \sum_{n=0}^{\infty} a_n k^{2n}$$

into (15.6.9) and solved an infinite system of nonlinear equations, to produce

(15.6.11) $$a_n = 2^{-2n}\binom{2n}{n}^2.$$

Then he recognized the series as that of an elliptic integral, to obtain

(15.6.12) $$\frac{1}{\mathrm{AGM}(1+k, 1-k)} = \frac{2}{\pi}\int_0^{\pi/2}\frac{dx}{\sqrt{1-k^2\sin^2 x}}.$$

This is a remarkable tour de force.

The function

(15.6.13) $$K(k) = \int_0^{\pi/2}\frac{dx}{\sqrt{1-k^2\sin^2 x}}$$

is the **elliptic integral of the first kind**. It can also be written in the algebraic form

(15.6.14) $$K(k) = \int_0^1 \frac{dt}{\sqrt{(1-t^2)(1-k^2t^2)}}.$$

In this notation, (15.6.9) becomes

(15.6.15) $$K(k^*) = (1+k)K(k).$$

This is the **Landen transformation** for the complete elliptic integral. J. Landen [**193**], the namesake of the transformation, studied related integrals: for example,

$$\kappa := \int_0^1 \frac{dx}{\sqrt{x^2(1-x^2)}} \ . \tag{15.6.16}$$

He derived identites such as

$$\kappa = \varepsilon\sqrt{\varepsilon^2 - \pi}, \quad \text{where } \varepsilon := \int_0^{\pi/2} \sqrt{2 - \sin^2\theta} \, d\theta \ , \tag{15.6.17}$$

proven mainly by suitable changes of variables in the integral for ε. In the paper by G. N. Watson [**307**], the reader will find a historical account of Landen's work, including the above identities.

The reader will find proofs in a variety of styles in the books by J. M. Borwein and P. B. Borwein [**71**] and H. McKean and V. Moll [**213**]. In trigonometric form, the Landen transformation states that

$$G(a,b) = \int_0^{\pi/2} \frac{d\theta}{\sqrt{a^2\cos^2\theta + b^2\sin^2\theta}} \tag{15.6.18}$$

is invariant under the change of parameters

$$(a,b) \mapsto \left(\tfrac{a+b}{2}, \sqrt{ab}\right).$$

D. J. Newman [**235**] presents a very clever proof: the change of variables $x = b\tan\theta$ yields

$$G(a,b) = \frac{1}{2}\int_{-\infty}^{\infty} \frac{dx}{\sqrt{(a^2+x^2)(b^2+x^2)}}. \tag{15.6.19}$$

Now let $x \mapsto x + \sqrt{x^2+ab}$ to complete the proof. Many of the above identities can now be searched for and proven on a computer; see the book by J. M. Borwein and D. H. Bailey [**69**].

Note 15.6.1. The reader will find a survey of the many aspects of Landen transformations in the paper by D. Manna and V. Moll [**209**]. As an intriguing open problem, the question of producing a Landen transformation for the integral

$$U_2^+(a,b,c) := \int_0^\infty \frac{dx}{ax^2+bx+c}$$

remains a challenge.

Note 15.6.2. The dynamics of the first two equations in (15.5.2) with initial data below the resolvent curve is quite complicated. Figure 15.6.1 shows the first 50000 iterates starting at $a = -5.0$ and $b = -20.4$.

Figure 15.6.2 shows 50000 iterates of the dynamics starting at $(-25.0, -2.4)$ and $(11.0, -13.7)$. These are identical to the naked eye.

Figure 15.6.3 shows 500000 iterates starting at $(11.0, -13.7)$. This figure illustrates the following conjecture by the author:

Conjecture 15.6.3. *The orbit of any point below the resolvent curve is dense in the open region below this curve.*

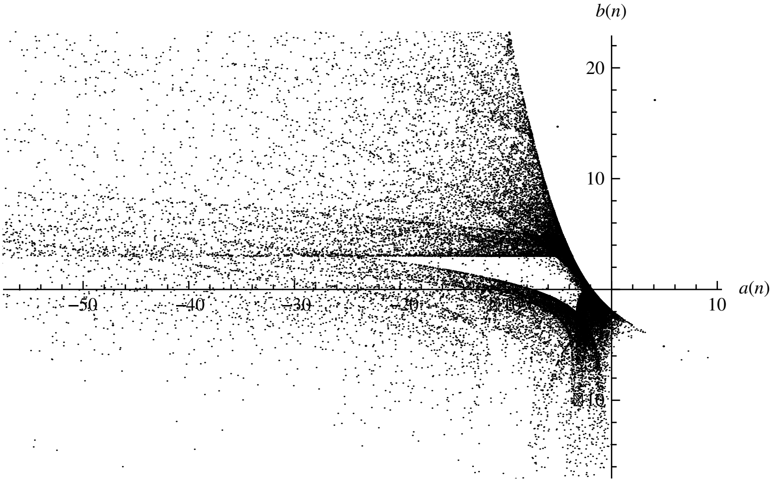


Figure 15.6.1. The dynamics below the resolvent curve.

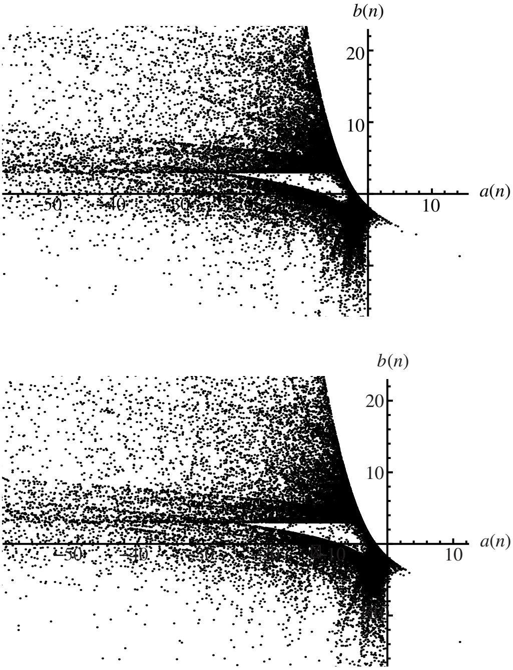


Figure 15.6.2. Two more examples of dynamics below the resolvent curve.

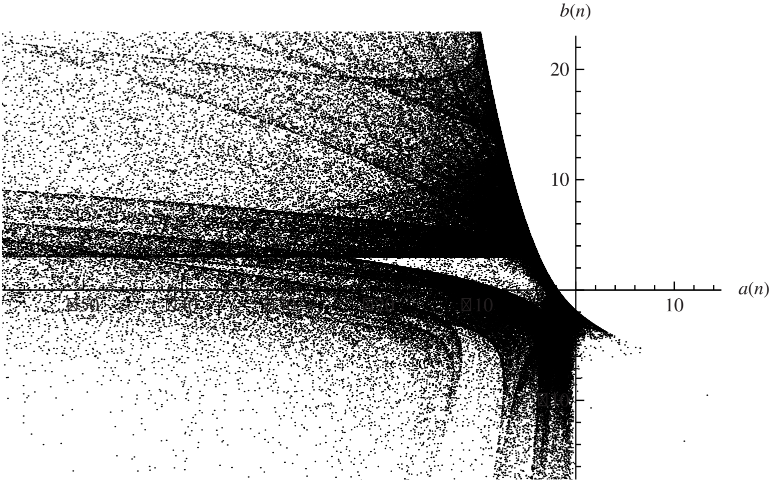


Figure 15.6.3. Illustration of the density conjecture.

Chapter 16

Three Special Functions: Γ, ψ, and ζ

16.1. Introduction

The subject of **Special Functions**, born with Euler in the eighteenth century, had a central role in the mathematics of the next century. Many functions were created to solve specific problems and a partial unified theory came from analysis in the form of **differential equations** and from algebra via the study of **group representations**. This last point of view will not be addressed here, but the classical reference is N. Ja. Vilenkin [**299**]. It requires more background than is assumed here, but keep it in mind for future reading. On the other hand, the Legendre and Chebyshev polynomials discussed in Chapter 14 are solutions of the **hypergeometric differential equation**

$$x(1-x)\frac{d^2y}{dx^2} + [c - (a+b+1)x]\,\frac{dy}{dx} - ab\,y(x) = 0.$$

The Hermite polynomials require the **confluent hypergeometric equation**

$$x\frac{d^2y}{dx^2} + (b-x)\,\frac{dy}{dx} - a\,y(x) = 0.$$

The reader will find a nice treatment of this point of view in the book by R. Beals and R. Wong [**43**].

In order to get a first understanding on how many special functions appear in the literature, the reader is encouraged to browse the magnificent **NIST Handbook of Mathematical Functions**, edited by F. W. J. Olver, D. W. Lozier, R. F. Boisvert, and C. W. Clark [**238**].

The goal in this final chapter is very modest. The reader is introduced to three interrelated functions. The first example is the **gamma function** $\Gamma(x)$ and its companion **beta function** $B(x, y)$, which extrapolate factorials and binomial coefficients to the complex plane and yield remarkable formulas such as

$$\left(\frac{1}{2}\right)! = \frac{\sqrt{\pi}}{2}. \tag{16.1.1}$$

The logarithmic derivative of $\Gamma(x)$, denoted by $\psi(x) = \Gamma'(x)/\Gamma(x)$, is the second function considered here. It is called the **digamma function**. Its special value $\psi(1) = -\gamma$ relates these functions to the Euler constant. Finally, the **Riemann zeta function** $\zeta(s)$ has profound connections to the distribution of prime numbers. The special value $\psi'(1) = \zeta(2) = \pi^2/6$ hints at the relation between these functions. An introduction to this connection is given here.

16.2. The gamma function

The traditional first course in differential equations usually contains an introduction to the **Laplace transform** and its applications. This is defined by

$$\mathfrak{L}(f(t)) := \int_0^\infty e^{-st} f(t)\, dt \tag{16.2.1}$$

for values of $s \in \mathbb{C}$ for which the integral is convergent. The identity $|e^{-st}| = e^{-t\, \mathrm{Re}\, s}$ shows that the region of convergence is always a half-plane of the form $\{s \in \mathbb{C} : \mathrm{Re}\, s > s_0\}$, for some $s_0 \in \mathbb{R}$ called the **abscissa of convergence**.

This transform is useful due to properties such as

$$\mathfrak{L}(f'(t)) = s\mathfrak{L}(f(t)) - f(0), \tag{16.2.2}$$

which convert differential equations into algebraic ones. One of the simplest examples is the Laplace transform of the function $f(t) = t^x$. This is expressed in terms of the gamma function defined next. Most of the discussion will assume only real values of the variables involved. The transition to complex arguments is usually painless.

Definition 16.2.1. The **gamma function** is defined by

$$\Gamma(x) = \int_0^\infty e^{-t} t^{x-1}\, dt. \tag{16.2.3}$$

The integral is convergent for $x > 0$. (Actually it converges for $\operatorname{Re} x > 0$, but only real arguments are considered here).

Exercise 16.2.2. Check that $\mathfrak{L}(t^x) = \Gamma(x+1)/s^{x+1}$.

Exercise 16.2.3. Prove that $\Gamma(x)$ is a continuous function of $x \in \mathbb{R}^+$.

16.3. Elementary properties of the gamma function

This section discusses some properties of the gamma function that are direct consequences of (16.2.3). The starting point is the **functional equation**.

Theorem 16.3.1. *The gamma function satisfies*

$$\Gamma(x+1) = x\Gamma(x). \tag{16.3.1}$$

Proof. Integrate by parts. □

This identity has a number of interesting consequences.

Corollary 16.3.2. *For $n \in \mathbb{N}$,*

$$n! = \Gamma(n+1). \tag{16.3.2}$$

Proof. The sequences $f_n = n!$ and $g_n = \Gamma(n+1)$ satisfy the same recurrence $a_{n+1} = na_n$ and have the same initial value $a_1 = 1$. □

Note 16.3.3. The previous corollary shows that $\Gamma(x)$ is an extension of factorials to positive real arguments x. For instance,

$$\left(\frac{1}{2}\right)! = \Gamma\left(\frac{3}{2}\right) = \int_0^\infty e^{-t} t^{-1/2}\, dt,$$

and

$$\left(\frac{1}{3}\right)! = \Gamma\left(\frac{4}{3}\right) = \int_0^\infty e^{-t} t^{1/3}\, dt.$$

The question of how to evaluate these integrals in terms of simpler expressions is quite complicated. For instance, how does one know that the first integral simplifies to produce (16.1.1) and that the second one does not simplify at all.

Corollary 16.3.4. *The gamma function* $\Gamma(x)$*, defined originally for* $x > 0$*, has an extension to* $\mathbb{R}$*. The only singularities are poles at the negative integers.*

Proof. The functional equation, written as

$$\Gamma(x) = \frac{\Gamma(x+1)}{x}, \tag{16.3.3}$$

gives the extension for $-1 < x < 0$. The computation

$$\lim_{x\to 0} x\,\Gamma(x) = \lim_{x\to 0} \Gamma(x+1) = 1 \tag{16.3.4}$$

shows that, near $x = 0$, the function $\Gamma(x) \sim 1/x$ so it has a pole at $x = 0$. Iterate this argument to obtain the result. □

Corollary 16.3.5. *Let* $k \in \mathbb{N}$ *and* $x \in \mathbb{R}$*. Then*

$$\Gamma(x+k) = \Gamma(x)(x)_k \tag{16.3.5}$$

where $(x)_k = x(x+1)\cdots(x+k-1)$ *is the Pochhammer symbol introduced in* (2.1.9)*.*

Proof. Fix $x \in \mathbb{R}$. Both sides of (16.3.5) satisfy the recurrence $a_{k+1} = (x+k)a_k$ and have the same initial value $a_0 = \Gamma(x)$. □

16.4. Special values of the gamma function

The functional equation has produced the values

$$\Gamma(n) = (n-1)! \tag{16.4.1}$$

for $n \in \mathbb{N}$. The next theorem states an important special value.

Theorem 16.4.1. *The gamma function satisfies*

$$\Gamma\left(\tfrac{1}{2}\right) = \sqrt{\pi}. \tag{16.4.2}$$

Proof. The change of variable $t = s^2$ yields

$$\Gamma\left(\tfrac{1}{2}\right) = \int_0^\infty e^{-t} t^{-1/2} dt = 2 \int_0^\infty e^{-s^2}\, ds.$$

This is the classical **normal integral** of basic statistics. Many proofs of the value

$$I := \int_0^\infty e^{-s^2}\, ds = \frac{\sqrt{\pi}}{2}$$

appear in the book by G. Boros and V. Moll [**65**]. A simple one is based on squaring the integral to produce

$$I^2 = \int_0^\infty e^{-x^2}\, dx \times \int_0^\infty e^{-s^2}\, ds.$$

Changing variables in the second integral produces

$$\begin{aligned} I^2 &= \int_0^\infty \int_0^\infty x e^{-x^2(1+y^2)}\, dx\, dy \\ &= \frac{1}{2} \int_0^\infty \frac{dx}{1+y^2} \\ &= \frac{1}{2} \tan^{-1} \infty, \end{aligned}$$

which gives the result. □

Exercise 16.4.2. Use (16.3.5) to establish the value

$$\Gamma\left(k + \tfrac{1}{2}\right) = \frac{(2k)!\,\sqrt{\pi}}{2^{2k}\, k!}$$

for $k \in \mathbb{N}$.

Exercise 16.4.3. Evaluate

$$J_n = \int_0^\infty x^n e^{-x^2}\, dx$$

and give a new solution of Exercise 3.8.9.

16.5. The infinite product for the gamma function

This section discusses a representation of the gamma function as an infinite product. The expression

$$G_n^*(x) = x \prod_{k=1}^{n} \left(1 + \frac{x}{k}\right) \tag{16.5.1}$$

gives a polynomial that vanishes at $x = 0$ and at the negative integers $x = -1, -2, \ldots, -n$. The goal is to let $n \to \infty$ to produce a function that vanishes at all negative integers and also at zero. The issue of convergence, discussed briefly in Note 12.12.8, shows that it is better to modify G_n^* and to consider instead

$$G_n(x) = x \prod_{k=1}^{n} \left(1 + \frac{x}{k}\right) e^{-x/k}. \tag{16.5.2}$$

To simplify the function G_n, write it as

$$G_n(x) = \frac{e^{-xH_n}}{n!} \prod_{k=0}^{n} (x+k) \tag{16.5.3}$$

where H_n is the harmonic number. The relation (16.3.5) now gives

$$G_n(x) = \frac{\Gamma(x+n+1)}{n!\,\Gamma(x)} e^{-xH_n}. \tag{16.5.4}$$

The behavior of H_n as $n \to \infty$ is described first. The next proposition is a restatement of Definition 13.7.6.

Proposition 16.5.1. *The limit*

$$\gamma := \lim_{n\to\infty} H_n - \ln n \tag{16.5.5}$$

*exists. It is called **Euler's constant**.*

Exercise 16.5.2. Give a direct proof of the existence of the limit by discussing the behavior of the sequence $a_n = H_n - \ln n$.

In order to compute the limit of $G_n(x)$ as $n \to \infty$, it is convenient to write it as

$$G_n(x) = \frac{\Gamma(x+n+1)}{n!\,\Gamma(x)\,n^x} e^{-x(H_n - \ln n)}. \tag{16.5.6}$$

Exercise 16.5.3. Use Stirling's formula to check that, for $x \in \mathbb{N}$,

$$\lim_{n \to \infty} \frac{\Gamma(x+n+1)}{n!\,n^x} = 1. \tag{16.5.7}$$

Note 16.5.4. The asymptotic behavior of the gamma function

$$\Gamma(z) \sim \sqrt{2\pi} z^{z-1/2} e^{-z}, \qquad \text{as } z \to \infty \text{ with } z > 0, \tag{16.5.8}$$

shows that the limit (16.5.7) is valid for $x \in \mathbb{R}$. The proof of (16.5.8) is obtained by **Laplace's method** outlined next. The reader will find in [**217**] a very nice introduction to asymptotic methods.

The goal is to describe the behavior of

$$I(\lambda) = \int_a^b f(t) e^{-\lambda g(t)}\, dt$$

as $\lambda \to \infty$. It is assumed that g has a strict minimum over $[a,b]$ at $c \in (a,b)$ with $g'(c) = 0$, $g''(c) > 0$, and $f(c) = 0$. The idea is that the main contribution to the value of $I(\lambda)$ comes from a small neighborhood of c. Then

$$\begin{aligned}
I(\lambda) &= e^{-\lambda g(c)} \int_a^b f(t) e^{-\lambda(g(t)-g(c))}\, dt \\
&\sim e^{-\lambda g(c)} f(c) \int_{c-\varepsilon}^{c+\varepsilon} e^{-\lambda(g(t)-g(c))}\, dt \\
&\sim e^{-\lambda g(c)} f(c) \int_{c-\varepsilon}^{c+\varepsilon} e^{-\lambda g''(c)(t-c)^2/2}\, dt \\
&\sim e^{-\lambda g(c)} f(c) \int_{-\infty}^{\infty} e^{-\lambda g''(c)(t-c)^2/2}\, dt \\
&= e^{-\lambda g(c)} f(c) \sqrt{\frac{2\pi}{\lambda g''(c)}}.
\end{aligned}$$

This method gives the stated asymptotic behavior for

$$\Gamma(z) = z^z \int_0^\infty e^{-z(t - \ln t)}\, dt. \tag{16.5.9}$$

Exercise 16.5.3 completes the proof of the product representation for the gamma function.

Theorem 16.5.5. *The gamma function satisfies*

$$\frac{1}{\Gamma(x)} = xe^{\gamma x} \prod_{k=1}^{\infty} \left(1 + \frac{x}{k}\right) e^{-x/k}. \tag{16.5.10}$$

Note 16.5.6. Observe that in (16.5.10) the function $1/\Gamma(x)$ appears in a factored format as is usually done for polynomials.

The next result establishes a connection between $\Gamma(x)$ and the trigonometric functions.

Corollary 16.5.7. *For $x \notin \mathbb{N}$, the* ***reflection formula***

$$\Gamma(x)\Gamma(1-x) = \frac{\pi}{\sin \pi x} \tag{16.5.11}$$

holds.

Proof. The result follows directly from (16.5.10) and the infinite product for the sine function given in Theorem 12.12.1. □

Exercise 16.5.8. Give an expression for $\Gamma\left(\frac{1}{3}\right)\Gamma\left(\frac{2}{3}\right)$ not involving the gamma function.

Exercise 16.5.9. Use the product for the gamma function to prove the **duplication formula**

$$\Gamma(2x) = \frac{1}{\sqrt{\pi}\, 2^{2x-1}} \Gamma(x)\Gamma\left(x + \tfrac{1}{2}\right). \tag{16.5.12}$$

Exercise 16.5.10. Use the product representation of the gamma function to establish the **multiplication formula**

$$\Gamma(x)\Gamma\left(x + \tfrac{1}{m}\right)\Gamma\left(x + \tfrac{2}{m}\right) \cdots \Gamma\left(x + \tfrac{m-1}{m}\right) = (2\pi)^{\frac{m-1}{2}} m^{\frac{1}{2} - mx} \Gamma(mx).$$

Exercise 16.5.11. Give an alternative solution of Exercise 16.5.8 using the multiplication rule.

Exercise 16.5.12. The infinite product for the gamma function can be employed to evaluate some infinite products. This exercise outlines one of them. Start with the product

$$P = \prod_{n=0}^{\infty} \frac{(n+a_1)(n+a_2)\cdots(n+a_r)}{(n+b_1)(n+b_2)\cdots(n+b_s)}.$$

Prove that the product diverges unless $r = s$, so there are the same number of factors top and bottom. Moreover, the coefficients $\{a_i\}$ and $\{b_j\}$ must satisfy

$$a_1 + a_2 + \cdots + a_r = b_1 + b_2 + \cdots + b_r.$$

Hint: Recall the criteria for convergence of an infinite product given in (12.12.6). Then rewrite P as

$$P = \frac{a_1 \cdots a_r}{b_1 \cdots b_r} \times \prod_{n=1}^{\infty} \frac{(1 + a_1/n)(1 + a_2/n) \cdots (1 + a_r/n)}{(1 + b_1/n)(1 + b_2/n) \cdots (1 + b_r/n)}.$$

Conclude that

$$P = \frac{\Gamma(b_1)\Gamma(b_2) \cdots \Gamma(b_r)}{\Gamma(a_1)\Gamma(a_2) \cdots \Gamma(a_r)}.$$

The results presented in the next two exercises are due to J. Sondow and H. Yi [**276**].

Exercise 16.5.13. The Wallis-type product

$$2 = \frac{2}{1}\frac{4}{3}\frac{4}{5}\frac{6}{7}\;\frac{10}{9}\frac{12}{11}\frac{12}{13}\frac{14}{15}\;\frac{18}{17}\frac{20}{19}\frac{20}{21}\frac{22}{23}\cdots$$

is obtained by writing the right-hand side as

$$P_1 = \prod_{n=0}^{\infty} \frac{(8n+2)(8n+4)(8n+4)(8n+6)}{(8n+1)(8n+3)(8n+5)(8n+7)}.$$

Evaluate the product in terms of gamma factors and use the reflection formula (16.5.11) to obtain the value $P_1 = 2$. The values

$$\sin\frac{\pi}{8} = \frac{1}{2}\sqrt{2 - \sqrt{2}} \quad \text{and} \quad \sin\frac{3\pi}{8} = \frac{1}{2}\sqrt{2 + \sqrt{2}} \tag{16.5.13}$$

would help in the simplification.

Exercise 16.5.14. Give a proof of the identity

$$\sqrt{2 - \sqrt{2}} = \frac{2}{3}\frac{6}{5}\frac{10}{11}\frac{14}{13}\;\frac{18}{19}\frac{22}{21}\cdots$$

using an argument similar to Exercise 16.5.13.

Note 16.5.15. E. Catalan [**93**] obtained the Wallis-type product

$$\frac{\pi}{2\sqrt{2}} = \frac{4}{3}\frac{4}{5}\frac{8}{7}\frac{8}{9}\;\frac{12}{11}\frac{12}{13}\cdots$$

and also a similar product for e:

$$e = \frac{2}{1}\left(\frac{4}{3}\right)^{1/2}\left(\frac{6}{5}\frac{8}{7}\right)^{1/4}\left(\frac{10}{9}\frac{12}{11}\frac{14}{13}\frac{16}{15}\right)^{1/8}\cdots;$$

N. Pippenger [**248**] produced

$$\frac{e}{2} = \left(\frac{2}{1}\right)^{1/2}\left(\frac{2}{3}\frac{4}{3}\right)^{1/4}\left(\frac{4}{5}\frac{6}{5}\frac{6}{7}\frac{8}{7}\right)^{1/8}\cdots.$$

A nice unified treatment of these products is given by J. Sondow and H. Yi in [**276**].

Note 16.5.16. The infinite product representation for the gamma function is now employed to relate it to the Euler constant γ. This is achieved by taking the logarithms in (16.5.10) to produce

$$-\ln\Gamma(x) = \ln x + \gamma x + \sum_{k=1}^{\infty}\left[\ln\left(1+\frac{x}{k}\right) - \frac{x}{k}\right]. \tag{16.5.14}$$

Differentiation now yields

$$\frac{\Gamma'(x)}{\Gamma(x)} = -\frac{1}{x} - \gamma + x\sum_{k=1}^{\infty}\frac{1}{k(x+k)}. \tag{16.5.15}$$

Theorem 16.5.17. *The Euler constant is* $\gamma = -\Gamma'(1)$.

Proof. The value $x=1$ in (16.5.15) gives

$$\Gamma'(1) = -1 - \gamma + \sum_{k=1}^{\infty}\frac{1}{k(k+1)}. \tag{16.5.16}$$

The result follows by computing the series by partial fractions. □

The next exercise gives the values of the derivative of Γ at the positive integers.

Exercise 16.5.18. Establish the value

$$\Gamma'(n+1) = n!\,(H_n - \gamma).$$

Hint: Use (16.3.5).

Certain special values of $\Gamma'(x)$ can be expressed in terms of elementary constants. The next exercise provides one.

Exercise 16.5.19. Use the duplication formula to obtain

$$\Gamma'\left(\frac{1}{2}\right) = -\sqrt{\pi}(\gamma + 2\ln 2).$$

Note 16.5.20. The number γ is one of the important constants of mathematics. As in the case of e and π, it also has its own book, written by J. Havil [**162**]. The question of the irrationality of γ has resisted all efforts: it remains an open problem.

The next exercises provide integral representations for γ, or depending on your point of view, they give evaluations of definite integrals in terms of the constant γ.

Exercise 16.5.21. Differentiate (16.2.3) to produce

$$\gamma = -\int_0^\infty e^{-t}\ln t\,dt.$$

Use this integral to produce

$$\gamma = -\int_0^1 \ln\ln\frac{1}{t}\,dt.$$

Exercise 16.5.22. Establish the evaluation

$$\int_0^\infty e^{-t^2}\ln t\,dt = -\frac{\sqrt{\pi}}{4}\left(\gamma + 2\ln 2\right).$$

16.6. The beta function

The **beta function** defined by

$$B(x,y) = \int_0^1 t^{x-1}(1-t)^{y-1}\,dt \tag{16.6.1}$$

is an essential companion to the gamma function. The fundamental relation between these two functions in stated next.

Theorem 16.6.1. *The functions beta and gamma are related by the* ***functional equation***

$$B(x,y) = \frac{\Gamma(x)\,\Gamma(y)}{\Gamma(x+y)}. \tag{16.6.2}$$

Proof. The proof employs the result of Exercise 16.2.2

$$\mathfrak{L}\left(t^{x-1}\right) = \Gamma(x)\, s^{-x} \tag{16.6.3}$$

and the basic property of the Laplace transform

$$\mathfrak{L}(f * g) = \mathfrak{L}(f) \cdot \mathfrak{L}(g) \tag{16.6.4}$$

for the **convolution** of two functions

$$(f * g)(t) = \int_0^t f(\tau) g(t-\tau)\, d\tau. \tag{16.6.5}$$

Exercise 16.6.2. Prove (16.6.4).

To prove the statement of the theorem, simply observe that

$$\begin{aligned}
\Gamma(x) s^{-x}\, \Gamma(y) s^{-y} &= \mathfrak{L}\left(\int_0^t \tau^{x-1}(t-\tau)^{y-1}\, d\tau \right) \\
&= \mathfrak{L}\left(t^{x+y-1} \int_0^1 u^{x-1}(1-u)^{y-1}\, du \right) \\
&= \mathfrak{L}\left(t^{x+y-1}\, B(x,y) \right) \\
&= \Gamma(x+y) s^{x+y}\, B(x,y).
\end{aligned}$$

The result follows from here. □

Several properties of the beta function are given as exercises.

Exercise 16.6.3. The beta function is symmetric: $B(x,y) = B(y,x)$. **Hint:** A simple change of variable in the integral representation for B does the trick. Of course, the result also follows from (16.6.1).

Exercise 16.6.4. Prove the integral representations

$$B(x,y) = \int_0^\infty \frac{t^{x-1}\, dt}{(1+t)^{x+y}} = \int_0^1 \frac{t^{x-1} + t^{y-1}}{(1+t)^{x+y}}\, dt. \tag{16.6.6}$$

Exercise 16.6.5. Prove the relation

$$\int_0^1 \frac{dx}{\sqrt{1-x^4}} \times \int_0^1 \frac{x^2\, dx}{\sqrt{1-x^4}} = \frac{\pi}{4}. \tag{16.6.7}$$

This is the **lemniscatic identity** of L. Euler [**121**]. The formula is a special case of an important identity of Legendre among the periods of an elliptic integral. See H. McKean and V. Moll [**213**, page 69] for details.

Exercise 16.6.6. Prove the trigonometric version of the beta integral

$$B(x,y) = 2\int_0^{\pi/2} \cos^{2x-1}\theta\, \sin^{2y-1}\theta\, d\theta. \tag{16.6.8}$$

Exercise 16.6.7. This exercise presents an alternative proof of the functional equation given in Theorem 16.6.1. Check the evaluation

$$\Gamma(x) = 2\int_0^\infty u^{2x-1}e^{-u^2}\, du \tag{16.6.9}$$

and then compute the product $\Gamma(x)\Gamma(y)$ in polar coordinates to obtain

$$\Gamma(x)\Gamma(y) = 4\int_0^{\pi/2} \cos^{2x-1}\theta\, \sin^{2y-1}\theta\, d\theta \times \int_0^\infty r^{2x+2y-1}e^{-r^2}\, dr.$$

Evaluate both integrals to obtain the result.

Exercise 16.6.8. This exercise reproduces Serret's proof of the duplication formula for the gamma function. Compute

$$\begin{aligned} B(x,x) &= \int_0^1 \left(u-u^2\right)^{x-1}\, du \\ &= \int_0^1 \left(\tfrac{1}{4} - (\tfrac{1}{2}-u)^2\right)^{x-1}\, du \\ &= 2\int_0^{1/2} \left(\tfrac{1}{4} - (\tfrac{1}{2}-u)^2\right)^{x-1}\, du. \end{aligned}$$

Change variables $u \mapsto (1-\sqrt{v})/2$ to evaluate the last integral as $2^{1-2x}B(\frac{1}{2},x)$ and complete the argument.

Exercise 16.6.9. Let $x \in \mathbb{R}^+$. Prove that

$$B(x,\tfrac{1}{2}) = \frac{\Gamma^2(x)\, 2^{2x-1}}{\Gamma(2x)}, \tag{16.6.10}$$

$$B(x+\tfrac{1}{2},\tfrac{1}{2}) = \frac{\pi}{x\, 2^{2x-1}} \cdot \frac{\Gamma(2x)}{\Gamma^2(x)}. \tag{16.6.11}$$

In the case of $x = n \in \mathbb{N}$ this can be written as

$$B(n,\tfrac{1}{2}) = \frac{2^{2n}}{n}\binom{2n}{n}^{-1} \quad \text{and} \quad B(n+\tfrac{1}{2},\tfrac{1}{2}) = \frac{\pi}{2^{2n}}\binom{2n}{n}.$$

Find an expression for $B(n, m+\frac{1}{2})$ and $B(n+\frac{1}{2}, m+\frac{1}{2})$.

16.7. The digamma function

The product representation for the sine function given in (12.12.1) is

$$\frac{\sin \pi x}{\pi x} = \prod_{k=1}^{\infty} \left(1 - \frac{x^2}{k^2} \right).$$

Ignoring issues of convergence, this product produces

$$\ln \sin \pi x - \ln \pi x = \sum_{k=1}^{\infty} \ln \left(1 - \frac{x^2}{k^2} \right).$$

Differentiation and a partial fraction expansion now give

$$\pi \cot \pi x - \frac{1}{x} = \sum_{k=1}^{\infty} \left(\frac{1}{x+k} + \frac{1}{x-k} \right).$$

Now observe that the series on the right contains all terms $1/(x+k)$ with $k \in \mathbb{Z}$, except $k = 0$. But, lucky enough, this has appeared on the left-hand side. This gives

$$\pi \cot \pi x = \sum_{k=-\infty}^{\infty} \frac{1}{x+k}. \tag{16.7.1}$$

This sum does not converge, so it has to be taken in the principal value sense; that is,

$$\pi \cot \pi x = \lim_{n \to \infty} \sum_{k=-n}^{n} \frac{1}{x+k}. \tag{16.7.2}$$

Exercise 16.7.1. Use (16.7.1) to check that $\cot \pi x$ is a periodic function of x with period 1.

The same procedure applied to the product representation of $\Gamma(x)$ gives an expression for the **digamma function** defined below.

Definition 16.7.2. The logarithmic derivative of the gamma function, called the **digamma function**, is defined by

$$\psi(x) = \frac{d}{dx} \ln \Gamma(x) = \frac{\Gamma'(x)}{\Gamma(x)}. \tag{16.7.3}$$

Note 16.7.3. Formula (16.5.14) gives

$$\psi(x) = -\frac{1}{x} - \gamma + x \sum_{k=1}^{\infty} \frac{1}{k(x+k)}. \tag{16.7.4}$$

The next series of exercises contains the main properties of the digamma function.

Exercise 16.7.4. Prove that

$$\psi(x+1) = \psi(x) + \frac{1}{x}$$

and

$$\psi(x) - \psi(1-x) = -\pi \cot \pi x.$$

Exercise 16.7.5. Use the value $\psi(1) = -\gamma$ to conclude that

$$\psi(n+1) = H_n - \gamma,$$

where $H_n = 1 + 1/2 + \cdots + 1/n$ is the harmonic number.

Exercise 16.7.6. Evaluate $\psi(1/2)$. Use it to establish the identity

$$\psi\left(n + \tfrac{1}{2}\right) = -\gamma - 2\ln 2 + 2\left(H_{2n} - \tfrac{1}{2}H_n\right).$$

Exercise 16.7.7. Prove the duplication formula

$$\psi(2x) = \frac{1}{2}\left(\psi(x) + \psi(x+1/2)\right) + \ln 2$$

and the extension

$$\psi(nx) = \frac{1}{n}\sum_{k=0}^{n-1} \psi\left(x + k/n\right) + \ln n.$$

Exercise 16.7.8. Establish the representation

$$\psi\left(\frac{x+1}{2}\right) - \psi\left(\frac{x}{2}\right) = 2\sum_{k=0}^{\infty} \frac{(-1)^k}{x+k}.$$

Note 16.7.9. Gauss gave a remarkable formula for the value of ψ at every rational number. The formula is stated for numbers in $(0,1)$. The values outside the unit interval are obtained using Exercise 16.7.4. Let p, $q \in \mathbb{N}$ with $p < q$. Then

$$\begin{aligned}\psi\left(\frac{p}{q}\right) &= -\gamma - \ln q - \frac{\pi}{2}\cot\left(\frac{\pi p}{q}\right) \\ &\qquad + \frac{1}{2}\sum_{k=1}^{q-1} \cos\left(\frac{2\pi k p}{q}\right) \ln\left(2 - 2\cos\left(\frac{2\pi k}{q}\right)\right).\end{aligned}$$

The reader will find a proof in the book by G. Andrews, R. Askey, and R. Roy [**18**].

16.8. The Riemann zeta function

In the computations of special values of the digamma function $\psi(x)$, the natural next step is to obtain expressions for the derivative $\psi'(x)$. Differentiation of the series (16.7.4) leads to

$$\psi'(x) = \sum_{k=0}^{\infty} \frac{1}{(x+k)^2}. \tag{16.8.1}$$

In particular,

$$\psi'(1) = \sum_{k=1}^{\infty} \frac{1}{k^2}. \tag{16.8.2}$$

In 1644 Pietro Mengoli asked for a closed-form expression for this sum and this search became known as the **Basel problem**. Its solution withstood the attack of the leading mathematicians of the time. The solution by the twenty-eight-year-old Leonhard Euler, in the form

$$\sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}, \tag{16.8.3}$$

brought him immediate recognition.

Euler established the value of

$$\sum_{n=1}^{\infty} \frac{1}{n^{2k}} \tag{16.8.4}$$

in terms of the Bernoulli numbers and in the next century B. Riemann introduced his remarkable function

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}. \tag{16.8.5}$$

In this language, Euler's solution to the Basel problem simply states the special value

$$\zeta(2) = \frac{\pi^2}{6}. \tag{16.8.6}$$

The function $\zeta(s)$ has profound control over the distribution of prime numbers. This is based on Euler's representation

$$\zeta(s) = \prod_{p \,\text{prime}} \frac{1}{1-p^{-s}}, \tag{16.8.7}$$

this being an analytic form of the fact that every natural number has a prime factorization.

The series defining $\zeta(s)$ converges for $\operatorname{Re} s > 1$ and Euler's product shows that $\zeta(s) \neq 0$ in this region. The relation between the zeros of $\zeta(s)$ and the distribution of primes is exemplified by the next theorem. This is the so-called **prime number theorem**.

Theorem 16.8.1. *The nth prime number is asymptotic to $n \ln n$.*

It turns out that this result is equivalent to the fact that $\zeta(s) \neq 0$ on the vertical line $\operatorname{Re} s = 1$. Riemann's work shows that the distribution of prime numbers is closely connected to his ζ-function and, in particular, to the location of its zeros. Based on numerical evidence, Riemann conjectured that all of them have to be on the vertical line $\operatorname{Re} s = \frac{1}{2}$. This is the famous **Riemann hypothesis**. A historical approach to $\zeta(s)$ may be found in the book by H. Edwards [**116**]. A nice description of current research appears in the paper by J. B. Conrey [**104**] and a possible alternative approach is in the paper by A. Granville [**147**].

16.9. The values of $\zeta(2n)$

Euler's proof of (16.8.6) is based on comparing the product representation and the Taylor series for $\sin x$. The product

$$\sin x = x \prod_{k=1}^{\infty} \left(1 - \frac{x^2}{k^2 \pi^2} \right) \tag{16.9.1}$$

is given in (12.12.1). To expand the product, it is necessary to form products taking one factor from each of the terms $1 - x^2/k^2\pi^2$. The contribution to the coefficient of x^2 comes from taking all terms 1 with one exception. Matching this to the coefficient of x^3 in the Taylor series (recall the extra x factor on the right) gives

$$-\frac{1}{3!} = -\left(\frac{1}{1^2\pi^2} + \frac{1}{2^2\pi^2} + \frac{1}{3^2\pi^2} + \cdots \right). \tag{16.9.2}$$

This is (16.8.6).

Exercise 16.9.1. Compute the coefficient of x^4 to obtain

$$\zeta(4) = \pi^4/90.$$

The values of $\zeta(2n)$ are provided next.

Theorem 16.9.2. *For any $n \in \mathbb{N}$,*

$$\zeta(2n) = \frac{(-1)^{n-1}B_{2n}}{2(2n)!}(2\pi)^{2n}. \tag{16.9.3}$$

Proof. The logarithm of the identity (16.9.1) is

$$\ln \sin x = \ln x + \sum_{k=1}^{\infty} \ln\left(1 - \frac{x^2}{k^2\pi^2}\right) \tag{16.9.4}$$

and differentiation produces

$$\cot x = \frac{1}{x} - \sum_{k=1}^{\infty} \frac{2x}{k^2\pi^2} \times \left(1 - \frac{x^2}{k^2\pi^2}\right)^{-1}. \tag{16.9.5}$$

Now recognize the geometric series

$$\left(1 - \frac{x^2}{k^2\pi^2}\right)^{-1} = \sum_{r=0}^{\infty} \frac{x^{2r}}{k^{2r}\pi^{2r}} \tag{16.9.6}$$

to obtain

$$\begin{aligned} \cot x &= \frac{1}{x} - 2x\sum_{k=1}^{\infty}\sum_{r=1}^{\infty} \frac{x^{2r-2}}{k^{2r}\pi^{2r}} \\ &= \frac{1}{x} - 2\sum_{r=1}^{\infty} \frac{\zeta(2r)}{\pi^{2r}} x^{2r-1}. \end{aligned}$$

Compare coefficients with those from the expansion (13.3.12)

$$\cot x = \sum_{n=0}^{\infty} (-1)^n \frac{2^{2n}}{(2n)!} B_{2n} x^{2n-1} \tag{16.9.7}$$

to obtain the result. □

The formula for $\zeta(2n)$ implies the result of Corollary 13.3.7.

Corollary 16.9.3. *The Bernoulli numbers satisfy $(-1)^{n-1}B_{2n} > 0$.*

Corollary 16.9.4. *For any $n \in \mathbb{N}$, the number $\dfrac{\zeta(2n)}{\pi^{2n}}$ is a rational number. In detail,*

$$\frac{\zeta(2n)}{\pi^{2n}} = \frac{2^{2n-1}\,|B_{2n}|}{(2n)!}.$$

Corollary 16.9.5. *The asymptotic behavior of the Bernoulli numbers is given by*

$$|B_{2n}| \sim \frac{2(2n)!}{(2\pi)^{2n}}.$$

The next corollary presents a lower bound for the Bernoulli numbers that shows the appearance of the interesting constant πe.

Corollary 16.9.6. *The Bernoulli numbers satisfy*

$$|B_{2n}| > 2\left(\frac{n}{\pi e}\right)^{2n}. \tag{16.9.8}$$

Proof. The bound $\zeta(2n) > 1$ gives

$$|B_{2n}| > 2\frac{(2n)!}{(2\pi)^{2n}}.$$

The result now follows from the next exercise. □

Exercise 16.9.7. Prove the bound $e^n > n^n/n!$.

16.10. Apéry's constant $\zeta(3)$

The last section of this book considers the **Apéry constant**

$$\zeta(3) = \sum_{n=1}^{\infty} \frac{1}{n^3} \tag{16.10.1}$$

with particular emphasis on its arithmetic properties. The goal of this section is to establish Apéry's theorem that $\zeta(3)$ is irrational. Historical information is provided at the end of the section.

The first proof follows some notes by B. Nica, available on line at

`math.arizona.edu/~savitt/teaching/nt/projects/nica.pdf`,

that are based on F. Beukers' proof of the result [**52**]. The proof begins with some elementary exercises and a proof that $\zeta(2) = \pi^2/6$ is irrational.

Exercise 16.10.1. Define

$$p_n(x) = \frac{1}{n!}\left(\frac{d}{dx}\right)^n \left[x^n(1-x)^n\right]. \tag{16.10.2}$$

Prove that $p_n(x)$ is a polynomial with integer coefficients. Express it in terms of the Legendre polynomials defined in (14.2.1).

Exercise 16.10.2. Expand the integrand as a geometric series and verify the identity

$$\int_0^1 \int_0^1 \frac{x^{r+a}\, y^{s+a}}{1-xy} dx\, dy = \sum_{n=0}^{\infty} \frac{1}{(n+r+a+1)(n+s+a+1)}.$$

In particular, take $r = s$ and $a = 0$ to obtain

$$\int_0^1 \int_0^1 \frac{x^r\, y^r}{1-xy} dx\, dy = \zeta(2) - \sum_{j=1}^{r} \frac{1}{j^2} = \zeta(2) + \frac{A_r}{d_r^2},$$

where $d_r = \mathrm{lcm}\{1, 2, \ldots, r\}$ and $A_r \in \mathbb{Z}$. Repeat the argument for the case $r > s$ and check that the sum has the same structure as in the case $r = s$.

Exercise 16.10.3. (a) Use the results of Exercises 16.10.1 and 16.10.2 to confirm that

$$\int_0^1 \int_0^1 \frac{p_n(x)(1-y)^n}{1-xy}\, dx\, dy = \frac{a_n + b_n \zeta(2)}{d_n^2}$$

for a_n, $b_n \in \mathbb{Z}$ and d_n as in Exercise 16.10.2.

(b) Integrate by parts to check the identity

$$\begin{aligned} J &:= \int_0^1 \int_0^1 \frac{p_n(x)(1-y)^n}{1-xy}\, dx\, dy \\ &= \int_0^1 \int_0^1 \left(\frac{x(1-x)y(1-y)}{1-xy} \right)^n \frac{dx\, dy}{1-xy} \end{aligned}$$

and conclude that $a_n + b_n \zeta(2) > 0$.

(c) Let $\varphi = (\sqrt{5} - 1)/2$ be the golden ratio. Prove that, for $0 \leq x, y \leq 1$, the inequality

$$\frac{x(1-x)y(1-y)}{1-xy} \leq \varphi^5 = \frac{5\sqrt{5} - 11}{2} < \frac{1}{10}$$

holds. **Hint:** Simply compute the maximum of the function.

Exercise 16.10.4. Let $\xi \in \mathbb{R}$ and assume there are integers a_n, b_n and a constant C such that

$$0 < |a_n + b_n \xi| < C\alpha^n \tag{16.10.3}$$

for some $0 < \alpha < 1$. Then ξ is irrational. **Hint:** Use Theorem 1.9.15.

These exercises provide an irrationality proof.

Theorem 16.10.5. *The value $\zeta(2) = \pi^2/6$ is irrational.*

Proof. The previous exercises give the bound

$$0 < |a_n + b_n\zeta(2)| < d_n^2\zeta(2)/10^n.$$

The bound $d_n < 3^n$ was established in Theorem 11.10.1. Now use the bound $|a_n + b_n\zeta(2)| < 2 \cdot (9/10)^n$ and Exercise 16.10.4. □

Note 16.10.6. The previous theorem complements Theorem 12.13.2, which states that π itself is irrational. The arithmetic character of π has been described in Theorem 12.13.8, where it is shown that π is transcendental. As a consequence of this result, all powers of π are irrational numbers. Therefore, so is $\zeta(2n)$, this being a rational multiple of π^{2n}. The question of the irrationality of the values of the Riemann zeta function at the odd integers became a natural one. This has shown itself to be a much harder problem to solve. It was first with caution and then with admiration that the mathematical community learned from R. Apéry that $\zeta(3)$ is irrational. The first proof presented below follows the ideas of Theorem 16.10.5. The second one is due to W. Zudilin and it has appeared in [**324**].

The methods developed by Apéry and others do not seem to apply to the other odd zeta values. On the other hand, some progress on this question has been achieved. K. Ball and T. Rivoal [**38, 254**] proved that there are infinitely many values $\zeta(2n+1)$ that are irrational. W. Zudilin [**323**] proved that one of the four numbers $\zeta(5)$, $\zeta(7)$, $\zeta(9)$, $\zeta(11)$ is irrational. It is conjectured that all of them are.

Theorem 16.10.7. *The Apéry constant $\zeta(3)$ is irrational.*

The next exercises will be employed in the proof.

Exercise 16.10.8. For $0 \leq x,\ y,\ w \leq 1$, define

$$f(x,y,w) = \frac{x(1-x)y(1-y)w(1-w)}{1-(1-xy)w}.$$

Then $f(x,y,w) \leq (\sqrt{2}-1)^4$.

Exercise 16.10.9. Let $r,\ s \in \mathbb{N}$. Define

$$g(r,s) = -\int_0^1 \int_0^1 \frac{x^r\, y^s\, \ln xy}{1-xy}\, dx\, dy.$$

Check that $g(r,r)$ has the form $2\zeta(3) + a_r/d_r^3$, where $d_r = \operatorname{lcm}\{1, 2, \ldots, r\}$ and $a_r \in \mathbb{Z}$. Also, for $r > s$, the number $g(r,s)$ has the form $a_{r,s}/d_r^3$. **Hint:** Differentiate with respect to a the relation

$$\int_0^1 \int_0^1 \frac{x^{r+a}\, y^{r+a}}{1-xy} dx\, dy = \sum_{n=0}^{\infty} \frac{1}{(n+r+a+1)^2}.$$

The case $r > s$ is treated by similar methods. Conclude that

$$\int_0^1 \int_0^1 \frac{-\ln xy}{1-xy}\, dx\, dy = 2\zeta(3).$$

Exercise 16.10.10. Let p_n be the polynomial defined in Exercise 16.10.1. Prove that

$$I_3 := -\int_0^1 \int_0^1 \frac{p_n(x)\, p_n(y)\, \ln xy}{1-xy}\, dx\, dy = \frac{a_n + b_n\zeta(3)}{d_n^3}$$

for some a_n, $b_n \in \mathbb{Z}$.

Proof of Apéry's theorem. Start with the expression

$$-\frac{\ln xy}{1-xy} = \int_0^1 \frac{dz}{1-(1-xy)z}$$

and substitute it into the integral I_3 in Exercise 16.10.10 to obtain

$$\begin{aligned}
|I_3| &= \left| \int_0^1 p_n(x) \left(\int_0^1 \int_0^1 \frac{p_n(y)\, dy\, dz}{1-(1-xy)z} \right) dx \right| \\
&= \left| \int_0^1 \frac{x^n(1-x)^n}{n!} \left(\int_0^1 \int_0^1 \frac{d^n}{dx^n} \left(\frac{p_n(y)\, dy\, dz}{1-(1-xy)z} \right) \right) dx \right| \\
&= \left| \int_0^1 \frac{x^n(1-x)^n}{n!} \left(\int_0^1 \int_0^1 \frac{(-1)^n n! p_n(y) y^n z^n}{(1-(1-xy)z)^{n+1}} dy\, dz \right) dx \right| \\
&= \left| \int_0^1 p_n(y) \left(\int_0^1 \int_0^1 \frac{x^n(1-x)^n y^n z^n}{(1-(1-xy)z)^{n+1}}\, dx\, dz \right) dy \right|.
\end{aligned}$$

Now make the change of variables

$$w = \frac{1-z}{1-(1-xy)z}$$

to obtain

$$\begin{aligned}|I_3| &= \left|\int_0^1 p_n(y)\left(\int_0^1\int_0^1 \frac{(1-x)^n(1-w)^n}{1-(1-xy)w}\,dx\,dw\right)dy\right| \\ &= \left|\int_0^1 \frac{y^n(1-y)^n}{n!}\left(\int_0^1\int_0^1 \frac{d^n}{dy^n}\left(\frac{(1-x)^n(1-w)^n}{1-(1-xy)w}\right)dx\,dw\right)dy\right| \\ &= \left|\int_0^1 \frac{y^n(1-y)^n}{n!}\left(\int_0^1\int_0^1 \frac{(-1)^n n!(1-x)^n(1-w)^n x^n w^n}{(1-(1-xy)w)^{n+1}}\,dx\,dw\right)dy\right| \\ &= \int_0^1\int_0^1\int_0^1 \left[\frac{x(1-x)y(1-y)w(1-w)}{1-(1-xy)w}\right]^n \frac{dx\,dy\,dw}{1-(1-xy)w}.\end{aligned}$$

This proves that the integral I_3 does not vanish. Exercise 16.10.8 gives the bound

$$\begin{aligned}|I_3| &= \left|\frac{a_n+b_n\zeta(3)}{d_n^3}\right| \leq (\sqrt{2}-1)^{4n}\int_0^1\int_0^1\int_0^1 \frac{dx\,dy\,dw}{1-(1-xy)w} \\ &= (\sqrt{2}-1)^{4n}\int_0^1\int_0^1 \frac{-\ln xy}{1-xy}\,dx\,dy = 2\zeta(3)(\sqrt{2}-1)^{4n},\end{aligned}$$

which leads to

$$0 < |a_n + b_n\zeta(3)| \leq 2\zeta(3)d_n^3\,(\sqrt{2}-1)^{4n}.$$

The bounds $d_n < 3^n$ and $27(\sqrt{2}-1)^4 < \frac{4}{5}$ imply

$$0 < |a_n + b_n\zeta(3)| \leq 2\zeta(3)(4/5)^n.$$

The last step employs Exercise 16.10.9. Exercise 16.10.4 shows that $\zeta(3)$ is irrational.

The second proof of Apéry's theorem presented here appears in the paper by W. Zudilin [**324**]. The argument is based on ideas that started in papers by L. A. Gutnik [**156**] and Yu. V. Nesterenko [**233**].

The starting point is the rational function

$$R_n(t) = \left(\frac{(t-1)(t-2)\cdots(t-n)}{t(t+1)\cdots(t+n)}\right)^2 \tag{16.10.4}$$

and the series

$$r_n := -\sum_{t=1}^{\infty} R_n'(t). \tag{16.10.5}$$

As before, $d_n = \operatorname{lcm}\{1, 2, \ldots, n\}$, with $d_0 = 1$ for completeness.

Lemma 16.10.11. *The series r_n is of the form $u_n\zeta(3) - v_n$ for some $u_n \in \mathbb{Z}$ and the rational number v_n satisfies $d_n^3 v_n \in \mathbb{Z}$.*

Proof. Square the partial fraction decomposition

$$\frac{(t-1)(t-2)\cdots(t-n)}{t(t+1)\cdots(t+n)} = \sum_{k=0}^{n} \frac{(-1)^{n-k}\binom{n+k}{n}\binom{n}{k}}{t+k}$$

to obtain

$$R_n(t) = \sum_{k=0}^{n} \left(\frac{A_{2,k}^{(n)}}{(t+k)^2} + \frac{A_{1,k}^{(n)}}{t+k} \right),$$

with

$$A_{2,k} = \binom{n+k}{n}^2 \binom{n}{k}^2 \in \mathbb{Z} \quad \text{and} \quad d_n A_{1,k} \in \mathbb{Z}. \tag{16.10.6}$$

Exercise 16.10.12. Check that

$$\sum_{k=0}^{n} A_{1,k} = 0. \tag{16.10.7}$$

Hint: Let f be a rational function. Evaluate the sum all its residues, including the pole at infinity. In the special case considered here, the rational function R_n is of order t^{-2} as $t \to \infty$; therefore its residue at infinity vanishes.

This yields

$$\begin{aligned} r_n &= \sum_{t=1}^{\infty} \sum_{k=0}^{n} \left(\frac{2A_{2,k}}{(t+k)^3} + \frac{A_{1,k}}{(t+k)^2} \right) \\ &= \sum_{k=0}^{n} \sum_{j=k+1}^{\infty} \left(\frac{2A_{2,k}}{j^3} + \frac{A_{1,k}}{j^2} \right) \\ &= 2\sum_{k=0}^{n} A_{2,k} \left(\zeta(3) - \sum_{j=1}^{k} \frac{1}{j^3} \right) - \sum_{k=0}^{n} \sum_{j=1}^{k} \frac{1}{j^2}. \end{aligned}$$

This has the desired form with

$$u_n = 2\sum_{k=0}^{n} A_{2,k} \tag{16.10.8}$$

and

$$v_n = 2\sum_{k=0}^{n} A_{2,k} \sum_{j=1}^{k} \frac{1}{j^3} + \sum_{k=0}^{n} A_{1,k} \sum_{j=1}^{k} \frac{1}{j^2}. \tag{16.10.9}$$

Exercise 16.10.13. Check that $d_n^3 v_n$ is an integer.

The proof of the lemma is complete. □

The next ingredient in the proof is provided by the magic of the WZ-method.

Lemma 16.10.14. *Define*

$$s_n(t) = -4(2n+1)(2t^2 - t - (2n+1)^2). \tag{16.10.10}$$

Then $S_n(t) = s_n(t)R_n(t)$ *satisfies*

$$(n+1)^3 R_{n+1}(t) - (2n+1)(17n^2+17n+5)R_n(t) + n^3 R_{n-1}(t) \\ = S_n(t+1) - S_n(t).$$

Exercise 16.10.15. Give a proof of Lemma 16.10.14.

The next result is obtained by differentiating the relation of Lemma 16.10.14 and summing over all $t \geq 1$.

Lemma 16.10.16. *The quantity* r_n *defined in* (16.10.5) *satisfies the recurrence*

$$(n+1)^3 r_{n+1} - (2n+1)(17n^2+17n+5)r_n + n^3 r_n = 0.$$

Proof. Sum over all t and observe that the right-hand side telescopes. The contributions at $t=1$ vanish as the reader will check in the next exercise. □

Exercise 16.10.17. Check that $R_n(t)$ and $S_n(t)$ have a zero at $t=1$ of multiplicity 2. Verify that the order of $R_n'(t)$ and $S_n'(t)$ at $t=\infty$ guarantees the validity of the argument.

The next step is to consider a second rational function, originally introduced by K. Ball [**38**] and T. Rivoal [**254**], by

$$\tilde{R}_n(t) = n!^2(2t+n)\frac{(t-1)\cdots(t-n)\cdot(t+n+1)\cdots(t+2n)}{[t(t+1)\cdots(t+n)]^4}$$

and the corresponding series

$$\tilde{r}_n := \sum_{t=1}^{\infty} \tilde{R}_n(t).$$

The plan is to show that $\tilde{r}_n = r_n$ by showing that it satisfies the recurrence established for r_n with the same initial conditions. Then, bounds on $\tilde{R}_n(t)$ will imply the estimates for r_n. In turn these will show that $\zeta(3)$ is irrational.

Exercise 16.10.18. Prove the following estimate for the product of n consecutive integers:

$$e^{-n}\frac{(m+n)^{m+n-1}}{m^{m-1}} < m(m+1)\cdots(m+n-1) < e^{-n}\frac{(m+n)^{m+n}}{m^m}.$$

Hint: Use the elementary inequalities

$$\frac{1}{m}\cdot\frac{(m+1)^m}{m^{m-1}} = \left(1+\frac{1}{m}\right)^m < e < \left(1+\frac{1}{m}\right)^{m+1} = \frac{1}{m}\cdot\frac{(m+1)^{m+1}}{m^m}.$$

The result of Exercise 16.10.18 is employed to estimate $\tilde{R}_n(t)$. For integer $t \geq 1$,

$$\begin{aligned}\tilde{R}_n(t)&\cdot\frac{(t+n)^5}{(2t+n)(t+2n)}\\ &= n!^2\cdot\frac{(t-1)\cdots(t-n)\cdot(t+n)\cdots(t+2n-1)}{\left[t(t+1)\cdots(t+n-1)\right]^4}\\ &< (n+1)^{2(n+1)}\cdot\frac{t^{5t-4}(t+2n)^{t+2n}}{(t-n)^{t-n}\,(t+n)^{5(t+n)-4}}.\end{aligned}$$

It follows that

$$\begin{aligned}\tilde{R}_n(t)&\cdot\frac{t^4(t+n)}{(2t+n)(t+2n)(n+1)^2}\\ &< (n+1)^{2n}\cdot\frac{t^{5t}(t+2n)^{t+2n}}{(t-n)^{t-n}\,(t+n)^{5(t+n)}}\\ &= \left(1+\frac{1}{n}\right)^{2n}\cdot e^{nf(t/n)}\\ &< e^2\left(\sup_{\tau>1} e^{f(\tau)}\right)^n,\end{aligned}$$

where

$$f(\tau) := \ln\frac{\tau^{5\tau}(\tau+2)^{\tau+2}}{(\tau-1)^{\tau-1}\,(\tau+1)^{5(\tau+1)}}. \tag{16.10.11}$$

Exercise 16.10.19. Verify that the only critical point of the function $f(\tau)$ in the region $\tau > 1$ is at

$$\tau_0 = -\frac{1}{2} + \sqrt{\frac{5}{4} + \sqrt{2}}.$$

Confirm that

$$\text{sup}_{\tau > 1} e^{f(\tau)} = f(\tau_0) = 4 \ln(\sqrt{2} - 1).$$

Hint: Use `Mathematica` or any symbolic language of your choice.

The bound for $\tilde{R}_n$ is stated next.

Lemma 16.10.20. *The function $\tilde{R}_n(t)$ satisfies the bound*

$$\tilde{R}_n(t) \cdot \frac{t^4(t+n)}{(2t+n)(t+2n)} < e^2(n+1)^2(\sqrt{2}-1)^{4n}.$$

The next exercise produces bounds for $\tilde{r}_n$ from those stated in Lemma 16.10.20

Exercise 16.10.21. Prove the estimate

$$\tilde{r}_n < 20(n+1)^4(\sqrt{2}-1)^{4n}.$$

Hint: Observe that in the series defining $\tilde{r}_n$ the first n terms vanish. Direct application of the bounds for $\tilde{R}_n(t)$ gives a bound involving $e^2(2\zeta(5) + 5n\zeta(4) + 2n^3\zeta(3))$. Check that this term is bounded from above by $20(n+1)^2$.

The final step is to show that $\tilde{r}_n = r_n$. The proof of the next lemma comes directly from the WZ-method applied to the rational function $\tilde{R}_n(t)$.

Lemma 16.10.22. *Define the polynomial*

$$\begin{aligned}Y_n(t) = -t^6 - (8n-1)t^5 &+ (4n^2+27n+5)t^4 + 2n(67n^2+71n+15)t^3 \\ &+ (358n^4 + 339n^3 + 76n^2 - 7n - 3)t^2 \\ &+ (384n^5 + 396n^4 + 97n^3 - 29n^2 - 17n - 2)t \\ &+ n(153n^5 + 183n^4 + 50n^3 - 30n^2 - 22n - 4)\end{aligned}$$

and the rational certificate

$$\tilde{S}_n(t) = \frac{Y_n(t)}{(2t+n)(t+2n-1)(t+2n)} \tilde{R}_n(t).$$

Then the identity

$$(n+1)\tilde{R}_{n+1}(t) - (2n+1)(17n^2+17n+5)\tilde{R}_n(t) + n^3\tilde{R}_{n-1}(t) \\ = \tilde{S}_n(t+1) - \tilde{S}_n(t)$$

holds.

Exercise 16.10.23. Confirm that $\tilde{r}_n$ satisfies the same recurrence as r_n. Then check the initial values and conclude that $\tilde{r}_n = r_n$.

Proof of Apéry's theorem. Lemma 16.10.11 shows that the term r_n has the form

$$r_n = u_n\zeta(3) - v_n, \tag{16.10.12}$$

with u_n, $d_n^3 v_n \in \mathbb{Z}$. If $\zeta(3) = p/q \in \mathbb{Q}$, then

$$0 < qr_n d_n^3 = pu_n d_n^3 - qd_n^3 v_n \tag{16.10.13}$$

is a positive integer. On the other hand, the bounds on $\tilde{r}_n = r_n$ give

$$0 < qr_n d_n^3 < 20q(n+1)^4 3^{3n}(\sqrt{2}-1)^{4n} = 20q(n+1)^4\left[27(\sqrt{2}-1)^4\right]^n.$$

The bound $27(\sqrt{2}-1)^4 < 4/5$ shows that the right-hand side converges to 0 as $n \to \infty$. This is gives a contradiction and the proof of Apéry's theorem is complete.

Bibliography

[1] J. C. Adams. Table of the first sixty-two numbers of Bernoulli. *JRAM*, 85:269–272, 1878.

[2] T. Agoh. On Giuga's conjecture. *Manuscripta Math.*, 87:501–510, 1995.

[3] M. Agrawal, N. Kayal, and N. Saxena. Primes is in P. *Ann. of Math.*, 160:781–793, 2004.

[4] M. Aigner. *Discrete Mathematics.* American Mathematical Society, 1st edition, 2007.

[5] W. R. Alford, A. Granville, and C. Pomerance. There are infinitely many Carmichael numbers. *Annals of Math.*, 139:703–722, 1994.

[6] U. Alfred. Primes which are factors of all Fibonacci sequences. *Fib. Quart.*, 2:33–38, 1964.

[7] J. Alvarez, M. Amadis, G. Boros, D. Karp, V. Moll, and L. Rosales. An extension of a criterion for unimodality. *Elec. Jour. Comb.*, 8:1–7, 2001.

[8] T. Amdeberhan, O. Espinosa, I. Gonzalez, M. Harrison, V. Moll, and A. Straub. Ramanujan's Master Theorem. *The Ramanujan Journal*, to appear, 2012.

[9] T. Amdeberhan, D. Manna, and V. Moll. The 2-adic valuation of a sequence arising from a rational integral. *Jour. Comb. A*, 115:1474–1486, 2008.

[10] T. Amdeberhan, D. Manna, and V. Moll. The 2-adic valuation of Stirling numbers. *Experimental Mathematics*, 17:69–82, 2008.

[11] T. Amdeberhan, L. Medina, and V. Moll. The integrals in Gradshteyn and Ryzhik. Part 5: Some trigonometric integrals. *Scientia*, 15:47–60, 2007.

[12] T. Amdeberhan, L. Medina, and V. Moll. Arithmetical properties of a sequence arising from an arctangent sum. *Journal of Number Theory*, 128:1808–1847, 2008.

[13] T. Amdeberhan and V. Moll. The integrals in Gradshteyn and Ryzhik. Part 7: Elementary examples. *Scientia*, 16:25–40, 2008.

[14] T. Amdeberhan, V. Moll, J. Rosenberg, A. Straub, and P. Whitworth. The integrals in Gradshteyn and Ryzhik. Part 9: Combinations of logarithmic, rational and trigonometric functions. *Scientia*, 17:27–44, 2009.

[15] T. Amdeberhan, V. Moll, and C. Vignat. The evaluation of a quartic integral via Schwinger, Schur and Bessel. *The Ramanujan Journal*, 28:1–14, 2012.

[16] R. Andre-Jeannin. Irrationalité de la somme des inverses de certaines suites récurrentes. *C. R. Acad. Sci. Paris Ser. I Math.*, 308:539–541, 1989.

[17] T. Andreescu and Z. Feng. *A Path to Combinatorics for Undergraduates*. Birkhäuser, Boston, 2004.

[18] G. Andrews, R. Askey, and R. Roy. *Special Functions*, volume 71 of *Encyclopedia of Mathematics and Its Applications*. Cambridge University Press, New York, 1999.

[19] G. Andrews and P. Paule. Some questions concerning computer-generated proofs of a binomial double-sum identity. *J. Symbolic Computation*, 11:1–7, 1994.

[20] G. E. Andrews. The death of proof? Semi-rigorous mathematics? you've got to be kidding! *The Mathematical Intelligencer*, 16:16–18, 1994.

[21] G. E. Andrews, Shalosh B. Ekhad, and D. Zeilberger. A short proof of Jacobi's formula for the number of representations of an integer as a sum of four squares. *Amer. Math. Monthly*, 100:273–276, 1993.

[22] J. Anglesio. Elementary problem 10292. *Amer. Math. Monthly*, 100:291, 1993.

[23] M. Apagodu. Series evaluation of a quartic integral. *The Ramanujan Journal*, 24:147–150, 2011.

[24] A. Apelblat. *Tables of Integrals and Series*. Verlag Harry Deutsch, Thun; Frankfurt am Main, 1996.

[25] R. Apéry. Irrationalité de $\zeta(2)$ et $\zeta(3)$. *Astérisque*, 61:11–13, 1979.

[26] T. Apostol. *Introduction to Analytic Number Theory*. Springer-Verlag, New York, 1976.

[27] T. Apostol. An elementary view of Euler's summation formula. *Amer. Math. Monthly*, 106:409–418, 1999.

[28] C. T. Aravnis. Hermite polynomials and quantum harmonic oscillator. *B. S. Math. Exchange*, 7:27–30, 2010.

[29] I. V. Artamkin. An elementary proof of the Miki-Zagier-Gessel identity. *Russ. Math. Surveys*, 64:1194–1195, 2007.

[30] E. Artin. *Collected Papers.* Addison Wesley, Reading, MA, 1965.

[31] M. Artin. *Algebra.* Prentice Hall, Englewood Cliffs, New Jersey, 1991.

[32] R. Azor, J. Gillis, and J. D. Victor. Combinatorial applications of Hermite polynomials. *SIAM J. Math. Anal.*, 13:879–890, 1982.

[33] D. H. Bailey, J. Borwein, A. Mattingly, and G. Wightwick. The computation of previous inaccesible digits of π^2 and Catalan's constant. *Preprint*, April 2011.

[34] D. H. Bailey and J. M. Borwein. Experimental mathematics: Examples, method and implications. *Notices Amer. Math. Soc.*, 52:502–514, 2005.

[35] D. H. Bailey and J. M. Borwein. Exploratory experimentation and computations. *Notices Amer. Math. Soc.*, 58:1410–1419, 2011.

[36] D. H. Bailey, J. M. Borwein, N. J. Calkin, R. Girgensohn, R. Luke, and V. Moll. *Experimental Mathematics in Action.* A. K. Peters, 1st edition, 2007.

[37] D. H. Bailey, P. Borwein, and S. Plouffe. On the rapid computation of various polylogarithmic constants. *Math. Comp.*, 66:903–913, 1997.

[38] K. Ball and T. Rivoal. Irrationalité d'une infinité de valeurs de la fonction zeta aux entiers impairs. *Invent. Math.*, 146:193–207, 2001.

[39] D. Baney, S. Beslin, and V. De Angelis. Farey tree and distribution of small denominators. In *Auburn University Top. Proc.*, pages 23–35, 1997.

[40] P. Barrucand. A combinatorial identity. *SIAM Review*, 17:168, 303–304, 1975.

[41] P. Bateman and H. Diamond. A hundred years of prime numbers. *Amer. Math. Monthly*, 103:729–741, 1996.

[42] M. Bayat. A generalization of Wolstenholme theorem. *Amer. Math. Monthly*, 104:557–560, 1997.

[43] R. Beals and R. Wong. *Special Functions. A Graduate Text*, volume 126 of *Cambridge Studies in Advanced Mathematics.* Cambridge University Press, New York, 2010.

[44] A. Beardon. *The Geometry of Discrete Groups*, volume 91 of *Graduate Texts in Mathematics.* Springer-Verlag, 1st edition, 1983.

[45] S. Beatty. Proof that e is not quadratically algebraic. *Amer. Math. Monthly*, 62:32–33, 1955.

[46] A. Benjamin and J. Quinn. *Proofs that Really Count. The Art of Combinatorial Proof*, The Mathematical Association of America, 2003.

[47] C. Bennett and E. Mosteig. On the collection of integers that index the fixed points of maps on the space of rational functions. In T. Amdeberhan and Victor H. Moll, editors, *Tapas in Experimental Mathematics*, volume 457 of *Contemporary Mathematics*, pages 53–67. American Mathematical Society, 2008.

[48] C. Berg and C. Vignat. Derivation of an integral of Boros and Moll via convolution of Student t-densities. *The Ramanujan Journal*, 27:147–150, 2012.

[49] B. Berndt. *Ramanujan's Notebooks, Part I.* Springer-Verlag, New York, 1985.

[50] B. Berndt and S. Bhargava. Ramanujan for lowbrows. *Amer. Math. Monthly*, 100:644–656, 1993.

[51] S. J. Beslin, D. J. Baney, and V. De Angelis. Small denominators: No small problem. *Math. Mag.*, 71:132–138, 1998.

[52] F. Beukers. A note on the irrationality of $\zeta(2)$ and $\zeta(3)$. *Bull. London Math. Soc.*, 11:268–272, 1979.

[53] E. Beyerstedt, V. Moll, and X. Sun. An analytic formula for the p-adic valuation of ASM numbers. *Journal of Integer Sequences*, 2011.

[54] Y. Bicheng and L. Debnath. Some inequalities involving the constant e, and an application to Carleman's inequality. *Jour. Math. Anal. Appl.*, 223:347–353, 1998.

[55] M. T. L. Bizley. Solution to advanced problem 5178. *Amer. Math. Monthly*, 72:203, 1964.

[56] J. L. Blue. A Legendre polynomial integral. *Math. Comp.*, 33:739–741, 1979.

[57] S. Boettner. *Mixed transcendental and algebraic extensions for the Risch-Norman algorithm.* PhD thesis, Tulane University, 2010.

[58] M. Bona. *A Walk Through Combinatorics.* World Scientific, New Jersey, 1st edition, 2002.

[59] G. Boros, M. Joyce, and V. Moll. A transformation of rational functions. *Elem. Math.*, 57:1–11, 2002.

[60] G. Boros, J. Little, E. Mosteig, V. Moll, and R. Stanley. A map on the space of rational functions. *Rocky Mountain Journal*, 35:1861–1880, 2005.

[61] G. Boros and V. Moll. A criterion for unimodality. *Elec. Jour. Comb.*, 6:1–6, 1999.

[62] G. Boros and V. Moll. An integral hidden in Gradshteyn and Ryzhik. *Jour. Comp. Applied Math.*, 106:361–368, 1999.

[63] G. Boros and V. Moll. A sequence of unimodal polynomials. *Jour. Math. Anal. Appl.*, 237:272–287, 1999.

[64] G. Boros and V. Moll. The double square root, Jacobi polynomials and Ramanujan's master theorem. *Jour. Comp. Applied Math.*, 130:337–344, 2001.

[65] G. Boros and V. Moll. *Irresistible Integrals.* Cambridge University Press, New York, 1st edition, 2004.

[66] G. Boros and V. Moll. Sums of arctangents and some formulas of Ramanujan. *Scientia*, 11:13–24, 2005.

[67] G. Boros, V. Moll, and J. Shallit. The 2-adic valuation of the coefficients of a polynomial. *Scientia, Series A*, 7:37–50, 2001.

[68] D. Borwein, J. M. Borwein, and R. Girgensohn. Giuga's conjecture on primality. *Amer. Math. Monthly*, 103:40–50, 1996.

[69] J. M. Borwein and D. H. Bailey. *Mathematics by Experiment: Plausible Reasoning in the* 21*-st Century.* A. K. Peters, 1st edition, 2003.

[70] J. M. Borwein, D. H. Bailey, and R. Girgensohn. *Experimentation in Mathematics: Computational Paths to Discovery.* A. K. Peters, 1st edition, 2004.

[71] J. M. Borwein and P. B. Borwein. *Pi and the AGM: A Study in Analytic Number Theory and Computational Complexity.* Wiley, New York, 1st edition, 1987.

[72] P. Borwein. *Computational Excursions in Analysis and Number Theory.* Springer Verlag, New York, 2002.

[73] A. Bostan and M. Kauers. The complete generating function for Gessel walks is algebraic. *Proc. Amer. Math. Soc.*, 138:3063–3078, 2010.

[74] M. Bousquet-Melou. Walks in the quarter plane: Kreweras' algebraic model. *Ann. Appl. Prob.*, 15:1451–1491, 2005.

[75] D. Bradley. Counting the positive rationals: A brief survey, September 2005. `http://arxiv.org/pdf/math/0509025`.

[76] P. Brändén. Iterated sequences and the geometry of zeros. *Crelle's Journal*, 658:115–131, 2012.

[77] F. Brenti. Log-concave and unimodal sequences in algebra, combinatorics and geometry: An update. *Contemporary Mathematics*, 178:71–89, 1994.

[78] D. Bressoud. *Proofs and Confirmations: The story of the Alternating Sign Matrix Conjecture*. Cambridge University Press, 1999.

[79] R. Breusch. Advanced problem 5178. *Amer. Math. Monthly*, 71:217, 1964.

[80] M. Bronstein. *Symbolic Integration I. Transcendental Functions*, volume 1 of *Algorithms and Computation in Mathematics.* Springer-Verlag, 1997.

[81] J. Brown and V. E. Hoggart. A primer for the Fibonacci sequence, part xvi. The central column sequence. *Fib. Quart.*, 16:41–46, 1978.

[82] R. Brualdi. *Introductory Combinatorics.* Prentice Hall, 4th edition, 2004.

[83] J. W. Bruce. A really trivial proof of the Lucas-Lehmer proof. *Amer. Math. Monthly*, 100:370–371, 1993.

[84] Y. A. Brychkov. *Handbook of Special Functions. Derivatives, Integrals, Series and Other Formulas.* Taylor and Francis, Boca Raton, Florida, 2008.

[85] R. L. Burden and D. Faires. *Numerical Analysis.* Brooks-Cole Pub. Co., 7th edition, 2001.

[86] E. B. Burger and R. Tubbs. *Making Transcendence Transparent.* Springer-Verlag, New York, 2004.

[87] T. S. Caley. A review of the von Staudt-Clausen theorem. Master's thesis, Dalhousie University, 2007.

[88] N. Calkin. A curious binomial identity. *Disc. Math.*, 131:335–337, 1994.

[89] N. Calkin and H. Wilf. Recounting the rationals. *Amer. Math. Monthly*, 107:360–363, 2000.

[90] D. Callan. A one-line description of the Calkin-Wilf enumeration of the rationals. 2005. `http://www.stat.wisc.edu/~callan/notes/enumerating_rationals/enumerating_rationals.pdf`.

[91] L. Carlitz. A theorem of Glaisher. *Canadian J. Math.*, 5:306–316, 1953.

[92] L. Carlitz. The sign of the Bernoulli and Euler numbers. *Amer. Math. Monthly*, 80:548–549, 1973.

[93] E. Catalan. Sur la constante d'Euler et la fonction de Binet. *C. R. Acad. Sci. Paris*, 77:198–201, 1873.

[94] M. Chamberland. An update on the $3x + 1$ problem, 2006. `http://www.cs.grinnell.edu/~chamberl/`.

[95] M. Chamberland and V. Moll. Dynamics of the degree six Landen transformation. *Discrete and Dynamical Systems*, 15:905–919, 2006.

[96] R. J. Chapman. Elementary problem 3375. *Amer. Math. Monthly*, 97:239–240, 1990.

[97] W. Y. C. Chen, Qing-Hu Hou, and Hai-Tao Jin. The Abel-Zeilberger algorithm. *Elec. Jour. Comb.*, 18:#P17, 2011.

[98] W. Y. C. Chen and E. X. W. Xia. 2-log-concavity of the Boros-Moll polynomials. *Proc. Edinburgh Math. Soc.*, to appear, 2012.

[99] W. Y. C. Chen and E. X. W. Xia. A proof of Moll's minimum conjecture. *European J. Combin.*, to appear, 2012.

[100] P. L. Chessin. A property of the coefficients of $(1+x)^{p-2}$. Elementary problem 1354. *Amer. Math. Monthly*, 66:727, 1959.

[101] G. Chrystal. *Algebra. Part II.* A. and C. Black, London, 2nd edition, 1922.

[102] H. Cohn. Problem 10457, submitted to the American Mathematical Monthly. *Amer. Math. Monthly*, 102:464, 1995. `http://research.microsoft.com/en-us/um/people/cohn/Papers/monthly.pdf`.

[103] H. Cohn. A short proof of the simple continued fraction expansion of e. *Amer. Math. Monthly*, 113:57–62, 2006.

[104] J. B. Conrey. The Riemann hypothesis. *Notices of the AMS*, 50:341–353, 2003.

[105] D. Cox. The arithmetic-geometric mean of Gauss. *L'Enseigement Mathematique*, 30:275–330, 1984.

[106] D. Cox. *Primes of the form* $x^2 + ny^2$. John Wiley and Sons, Inc., New York, 1st edition, 1989.

[107] T. W. Cusick. Recurrences for sums of powers of binomial coefficients. *Jour. Comb. Theory, Series A*, 52:77–83, 1989.

[108] D. P. Dalzell. On 22/7 and 355/113. *Eureka; the Archimedeans' journal*, 34:10–13, 1971.

[109] E. Deeba and D. Rodriguez. Stirling's series and Bernoulli numbers. *Amer. Math. Monthly*, 98:423–426, 1991.

[110] E. Deutsch and B. Sagan. Congruences for Catalan and Motzkin numbers and related sequences. *Jour. Number Theory*, 117:191–215, 2006.

[111] D. Dimitrov. Asymptotics of zeros of polynomials arising from rational integrals. *Jour. Math. Anal. Appl.*, 299:127–132, 2004.

[112] D. Dominici. Variations on a theme by Stirling. *Note Mat.*, 28:1–13, 2008.

[113] G. Dresden. Two irrational numbers from the last non-zero digits of $n!$ and n^n. *Math. Mag.*, 74:316–320, 2001.

[114] G. Dresden. Three transcendental numbers from the last non-zero digits of n^n, F_n, and $n!$. *Math. Mag.*, 81:96–105, 2008.

[115] G. V. Dunne. Bernoulli number identities from Quantum Field Theory. 2004. `http://arxiv.org/pdf/math.NT/0406610.pdf`.

[116] H. Edwards. *Riemann's Zeta Function.* Academic Press, New York, 1974.

[117] J. Edwards. *A treatise on the Integral Calculus*, volume I. MacMillan, New York, 1922.

[118] J. Edwards. *A treatise on the Integral Calculus*, volume II. MacMillan, New York, 1922.

[119] P. Erdős and S. Wagstaff. The fractional parts of the Bernoulli numbers. *Illinois Jour. Math.*, 24:104–112, 1980.

[120] H. Ebbinhaus et al. *Numbers*. Springer-Verlag, 2nd edition, 1995.

[121] L. Euler. De miris proprietatibus curvae elasticae sub aequatione $y = \int xx/\sqrt{1-x^4}\,dx$ contentae. Comment 605 enestroemianus index. In *Opera Omnia*, volume 21 of *I*, pages 91–118. Teubner, Berlin, 1924.

[122] L. Euler. *Introductio in Analysis Infinitorum.* English translation, *Introduction to Analysis of the Infinite*, by J. D. Blantan, Editor. Springer-Verlag, New York, 1st edition, 1988.

[123] S. Even and J. Gillis. Derangements and Laguerre polynomials. *Math. Proc. Camb. Phil. Soc.*, 79:135–143, 1976.

[124] C. Faber and R. Pandharipande. Logarithmic series and Hodge integrals in the tautological ring. *Michigan Math. J.*, 48:215–252, 2000.

[125] D. B. Fairlie and A. P. Veselov. Faulhaber and Bernoulli polynomials and solitions. *Physica D*, 152-153:47–50, 2001.

[126] M. Filaseta. Notes for a course in Transcendental Number Theory. 2011. `http://www.math.sc.edu/~filaseta/gradcourses/Math785/Math785Notes6.pdf`.

[127] B. Fine and G. Rosenberger. *The Fundamental Theorem of Algebra.* Undergraduate Texts in Mathematics. Springer-Verlag, 1997.

[128] B. Fine and G. Rosenberger. *Number Theory. An Introduction via the Distribution of Primes.* Birkhäuser, 2007.

[129] S. Fisk. Questions about determinants and polynomials. `arXiv:0808,1850`.

[130] J. Franel. Comments on question 42 by Laisant. *L'Intermediaire des Mathematiciens*, 1:45–47, 1894.

[131] J. Franel. Comments on question 170 by Laisant. *L'Intermediaire des Mathematiciens*, 2:33–35, 1895.

[132] D. Galvin. Erdös's proof of Bertrand's postulate, April-2006. `http://nd.edu/~dgalvin1/pdf/bertrand.pdf`.

[133] K. F. Gauss. Arithmetisch Geometrisches Mittel. *Werke*, 3:361–432, 1799.

[134] I. Gessel. Generalized rook polynomials and orthogonal polynomials. In D. Stanton, editor, *q-Series and Partitions*, volume 18 of *The IMA Volumes in Mathematics and Its Applications*, pages 159–176. Springer-Verlag, 1989.

[135] I. Gessel. Wolstenholme revisited. *Amer. Math. Monthly*, 105:657–658, 1998.

[136] I. Gessel. On Miki's identity for Bernoulli numbers. *Jour. Number Theory*, 110:75–82, 2005.

[137] G. Giuga. Su una presumibile proprietà caratteristica dei nummeri primi. *Ist. Lombardo Sci. Lett. Rend. A*, 83:511–528, 1950.

[138] J. W. L. Glaisher. A theorem in trigonometry. *Quart. J. Pure Appl. Math.*, 15:151–157, 1878.

[139] I. J. Good. A reciprocal Fibonacci series. *Fib. Quart.*, 12:346, 1974.

[140] R. W. Gosper Jr. Decision procedure for indefinite hypergeometric summation. *Proc. Natl. Acad. Sci. USA*, 75:40–42, 1978.

[141] X. Gourdon and B. Salvy. Computing one million digits of $\sqrt{2}$. *Rapport Technique, INRIA*, 155:1–6, 1993.

[142] F. Gouvea. *p-adic numbers.* Springer Verlag, 2nd edition, 1997.

[143] T. Gowers, editor. *The Princeton Companion to Mathematics.* Princeton University Press, 2008.

[144] I. S. Gradshteyn and I. M. Ryzhik. *Table of Integrals, Series, and Products.* Edited by A. Jeffrey and D. Zwillinger. Academic Press, New York, 7th edition, 2007.

[145] R. Graham, D. Knuth, and O. Patashnik. *Concrete Mathematics.* Addison Wesley, Boston, 2nd edition, 1994.

[146] A. Granville. It is easy to determine whether a given integer is prime. *Bull. Amer. Math. Soc.*, 42:3–38, 2005.

[147] A. Granville. Different approaches to the distribution of primes. *Milan J. Math.*, 78:1–25, 2009.

[148] R. Greene and S. Krantz. *Function Theory of One Complex Variable*, volume 40 of *Graduate Studies in Mathematics.* American Mathematical Society, 2002.

[149] W. E. Greig. Series of Fibonacci reciprocals. *Fib. Quart.*, 15:46–48, 1977.

[150] C. C. Grosjean. Some new integrals arising from mathematical physics, I. Bull. Belgian Math. Soc., *Simon Stevin*, 40:49–72, 1966.

[151] C. C. Grosjean. Some new integrals arising from mathematical physics, II. Bull. Belgian Math. Soc., *Simon Stevin*, 41:219–251, 1967.

[152] C. C. Grosjean. Some new integrals arising from mathematical physics, III. Bull. Belgian Math. Soc., *Simon Stevin*, 43:3–46, 1967.

[153] C. C. Grosjean. Some new integrals arising from mathematical physics, IV. Bull. Belgian Math. Soc., *Simon Stevin*, 45:321–383, 1972.

[154] M. P. Grosset and A. P. Veselov. Bernoulli numbers and solitions. *Journal of Nonlinear Physics*, 12:469–474, 2005.

[155] J. Gurland. On Wallis' formula. *Amer. Math. Monthly*, 63:643–645, 1956.

[156] L. A. Gutnik. Irrationality of some quantities that contain $\zeta(3)$. *Acta Arith.*, 43:255–264, 1983.

[157] D. Hanson. On the product of primes. *Canad. Math. Bull.*, 15:33–37, 1972.

[158] G. H. Hardy. *The Integration of Functions of a Single Variable*, volume 2 of *Cambridge University Tracts in Mathematical Physics*. Cambridge University Press, New York, N.Y., 2nd edition, 1958.

[159] G. H. Hardy, J. E. Littlewood, and G. Polya. *Inequalities*. Cambridge University Press, 2nd edition, 1951.

[160] G. H. Hardy, E. M. Wright; revised by D. R. Heath-Brown and J. Silverman. *An Introduction to the Theory of Numbers*. Oxford University Press, 6th edition, 2008.

[161] A. Hatcher. *The topology of numbers*. 2011. `http://www.math.cornell.edu/~hatcher/#TN`.

[162] J. Havil. *Gamma: Exploring Euler's Constant*. Princeton University Press, 1st edition, 2003.

[163] Y. Hellegouarch. *Introduction to the Mathematics of Fermat-Wiles*. Academic Press, New York, 2002.

[164] M. J. Hellman. A unifying technique for the solution of the quadratic, cubic, and quartic. *Amer. Math. Monthly*, 65:274–276, 1958.

[165] M. J. Hellman. The insolvability of the quintic re-examined. *Amer. Math. Monthly*, 66:410, 1959.

[166] C. Hermite. Sur l'integration des fractions rationelles. *Nouvelles Annales de Mathematiques (*2^{eme} *serie)*, 11:145–148, 1872.

[167] C. Hermite. Sur la fonction exponentielle. *C. R. Acad. Sci. Paris*, 77:74–79 and 226–233, 1873.

[168] O. Hijab. *Introduction to Calculus and Classical Analysis*. Springer-Verlag, New York, 1st edition, 1997.

[169] M. Hirschhorn. Calkin's binomial identity. *Disc. Math.*, 159:273–278, 1996.

[170] M. Hirschhorn. A note on partial fractions. *Austral. Math. Gazette*, 30:81, 2003.

[171] M. Hirschhorn. An interesting integral. *Math. Gazette*, 95:90–91, 2011.

[172] M. E. Hoffman. Derivative polynomials for tangent and secant. *Amer. Math. Monthly*, 102:23–30, 1995.

[173] M. E. Hoffman. Derivative polynomials, Euler polynomials, and associated integer sequences. *Elec. Jour. Comb.*, 6:#R21, 13 pages, 1999.

[174] V. E. Hoggatt Jr. *The Fibonacci and Lucas numbers.* Houghton Mifflin, 1969.

[175] V. E. Hoggatt Jr. Roots of Fibonacci polynomials. *Fib. Quart.*, 11:271–274, 1973.

[176] E. Horowitz. Algorithms for partial fraction decomposition and rational function integration. *Proc. of SYMSAM'71, ACM Press*, pages 441–457, 1971.

[177] D. Huylebrouck. Similarities in irrationality proofs for π, $\ln 2$, $\zeta(2)$, and $\zeta(3)$. *Amer. Math. Monthly*, 108:222–231, 2001.

[178] K. Ireland and M. Rosen. *A Classical Introduction to Number Theory.* Springer-Verlag, 2nd edition, 1990.

[179] J. H. Jaroma. Note on the Lucas-Lehmer test. *Irish. Math. Soc. Bull.*, 54:63–72, 2004.

[180] M. Kauers and P. Paule. A computer proof of Moll's log-concavity conjecture. *Proc. Amer. Math. Soc.*, 135:3837–3846, 2007.

[181] M. Kauers and P. Paule. *The Concrete Tetrahedron. Symbolic Sums, Recurrence Equations, Generating Functions, Asymptotic Estimates.* Springer-Verlag, Wien-New York, 2011.

[182] P. M. Kayll. Integrals don't have anything to do with discrete math, do they? *Math. Mag.*, 84:108–119, 2011.

[183] B. C. Kellner. The equation $\text{denom}(B_n) = n$ has only one solution. 2011. `http://www.bernoulli.org/~bk/denombneqn.pdf`.

[184] B. C. Kellner. The equivalence of Giuga's and Agoh's conjectures. 2011. `http://www.bernoulli.org/~bk/equivalence.pdf`.

[185] O. Knill. *Probability and Stochastic Processes with Applications.* Available from the author's website, 2011.

[186] T. Koshy. *Fibonacci and Lucas Numbers and Applications.* Pure and Applied Mathematics. John Wiley and Sons, Inc., New York, 2001.

[187] C. Koutschan and V. Levandovskyy. Computing one of Victor Moll's irresistible integrals with computer algebra. *Computer Science Journal of Moldova*, 16:35–49, 2008.

[188] J. Kramer and V. E. Hoggatt Jr. Special cases of Fibonacci periodicity. *Fib. Quart.*, 10:519–522, 1972.

[189] J. C. Lagarias. The $3x + 1$ problem and its generalizations. *Amer. Math. Monthly*, 92:3–23, 1985.

[190] J. C. Lagarias. The $3x + 1$ problem: An annotated bibliography. arXiv:math.NT/0309224, v5, 5 Jan. 2006.

[191] J. H. Lambert. Mémoire sur quelques propriétés remarquables des quantités transcendentes circulaires et logarithmiques. *Histoire de l'Academie, Berlin*, XVII:265–322, 1768.

[192] E. Landau. *Differential and Integral Calculus.* Chelsea Publishing Company, 3rd edition, 1980.

[193] J. Landen. An investigation of a general theorem for finding the length of any arc of any conic hyperbola, by means of two elliptic arcs, with some other new and useful theorems deduced therefrom. *Philos. Trans. Royal Soc. London*, 65:283–289, 1775.

[194] L. J. Lange. An elegant continued fraction for π. *Amer. Math. Monthly*, 106:456–458, 1999.

[195] M. E. Larsen. *Summa Summarum.* CRM Treatises in Mathematics. Canadian Mathematical Society, Ottawa, Ontario, and A. K. Peters, Wellesley, Massachusetts, 2007.

[196] S. Lattés. Sur l'iteration des substitutions rationelles et les fonctions de Poincaré. *C. R. Acad. Sci. Paris*, 166:26–28, 1918.

[197] D. Lazard and R. Rioboo. Integration of rational functions: Rational computation of the logarithmic part. *Journal of Symbolic Computation*, 9:113–116, 1990.

[198] A. M. Legendre. *Théorie des Nombres.* Firmin Didot Frères, Paris, 1830.

[199] T. Lengyel. The order of the Fibonacci and Lucas numbers. *Fib. Quart.*, 33:234–239, 1995.

[200] J. Liouville. Addition à la note sur l'irrationnalité du nombre e. *J. Math. Pures Appl.*, 5:193–194, 1840.

[201] J. Little. On the zeroes of two families of polynomials arising from certain rational integrals. *Rocky Mountain Journal*, 35:1205–1216, 2005.

[202] M. Livio. *The Golden Ratio: The Story of PHI, the World's Most Astonishing Number.* Broadway Books, 2002.

[203] S. L. Loney. *Plane Trigonometry, Part II.* Cambridge University Press, 1893.

[204] L. Lorentzen and H. Waadeland. *Continued Fractions with Applications.* North-Holland, Amsterdam, The Netherlands, 1992.

[205] S. K. Lucas. Approximations to π derived from integrals with nonnegative integrands. *Amer. Math. Monthly*, 116:166–172, 2009.

[206] R. S. Luthar and W. C. Waterhouse. A generalization of Wilson's theorem. Elementary problem E1603. *Amer. Math. Monthly*, 71:434, 1964.

[207] K. MacMillan and J. Sondow. Proofs of power sum and binomial coefficient congruences via Pascal's identity. *Amer. Math. Monthly*, 118:549–551, 2011.

[208] D. Manna and V. Moll. A simple example of a new class of Landen transformations. *Amer. Math. Monthly*, 114:232–241, 2007.

[209] D. Manna and V. Moll. Landen Survey. *MSRI Publications: Probabilty, Geometry and Integrable Systems. In Honor of Henry McKean's* 75*th Birthday*, 55:201–233, 2008.

[210] E. Maor. *e. The Story of a Number.* Princeton University Press, New Jersey, 1994.

[211] R. J. McIntosh. A necessary and sufficient condition for the primality of Fermat numbers. *Amer. Math. Monthly*, 90:98–99, 1983.

[212] R. J. McIntosh and E. L. Roettger. A search for Fibonacci-Wieferich and Wolstenholme primes. *Math. Comp.*, 76:2087–2094, 2007.

[213] H. McKean and V. Moll. *Elliptic Curves: Function Theory, Geometry, Arithmetic.* Cambridge University Press, New York, 1997.

[214] P. R. McNamara and B. Sagan. Infinite log-concavity: Developments and conjectures. *Adv. Appl. Math.*, 94:79–96, 2010.

[215] L. Medina and E. Rowland. p-regularity of the p-adic valuation of the Fibonacci sequence. *Submitted for publication*, preprint, 2011.

[216] H. Miki. A relation between Bernoulli numbers. *J. Number Theory*, 10:297–302, 1978.

[217] P. D. Miller. *Applied Asymptotic Analysis*, volume 75 of *Graduate Studies in Mathematics.* American Mathematical Society, 2006.

[218] S. J. Miller and R. Takloo-Bighash. *An Invitation to Modern Number Theory.* Princeton University Press, 2006.

[219] S. Minsker. A familiar combinatorial identity proved by complex analysis. *Amer. Math. Monthly*, 80:1051, 1973.

[220] S. P. Mohanty. The number of primes is infinite. *Fib. Quart.*, 16:381–384, 1978.

[221] V. Moll. The evaluation of integrals: A personal story. *Notices of the AMS*, 49:311–317, 2002.

[222] V. Moll. The integrals in Gradshteyn and Ryzhik. Part 13: Trigonometric forms of the beta function. *Scientia*, 19:91–96, 2010.

[223] L. Mordell. The sign of the Bernoulli numbers. *Amer. Math. Monthly*, 80:547–548, 1973.

[224] F. Morley. Note on the congruence $2^{4n} \equiv (-1)^n(2n)!/(n!)^2$, where $2n+1$ is a prime. *Ann. Math.*, 9:168–170, 1894–1895.

[225] Y. Moschovakis. *Notes on Set Theory.* Undergraduate Texts in Mathematics. Springer-Verlag, New York, 1st edition, 2005.

[226] E. Mosteig. Fixed points of maps on the space of rational functions. *Online Journal of Analytic Combinatorics*, 1:1–9, 2006.

[227] K. Motose. Rational values of trigonometric functions. *Amer. Math. Monthly*, 114:218, 2007.

[228] D. Mumford. *Tata Lectures on Theta, II*, volume 43 of *Progr. Math.* Birkhäuser, Boston, 1984.

[229] M. R. Murty. Artin's conjecture for primitive roots. *The Mathematical Intelligencer*, 11:59–67, 1988.

[230] M. R. Murty. *Introduction to p-adic Analytic Number Theory*, volume 27 of *Studies in Advanced Mathematics.* American Mathematical Society, 1st edition, 2002.

[231] P. Nahim. *An Imaginary Tale. The Story of* $\sqrt{-1}$. Princeton University Press, 1998.

[232] G. Nemes. On the coefficients of the asymptotic expansion of $n!$. *Journal of Integer Sequences*, 13: Article 10.6.6, 2010.

[233] Yu. V. Nesterenko. A few remarks on $\zeta(3)$. *Mat. Zametki [Math. Notes]*, 59:865–880, 1996.

[234] D. J. Newman. Simple analytic proof of the Prime Number Theorem. *Amer. Math. Monthly*, 87:693–696, 1980.

[235] D. J. Newman. A simplified version of the fast algorithm of Brent and Salamin. *Math. Comp.*, 44:207–210, 1985.

[236] I. Niven. The transcendence of π. *Amer. Math. Monthly*, 46:469–471, 1939.

[237] I. Niven. A simple proof that π is irrational. *Bull. Amer. Math. Soc.*, 53:509, 1947.

[238] F. W. J. Olver, D. W. Lozier, R. F. Boisvert, and C. W. Clark, editors. *NIST Handbook of Mathematical Functions.* Cambridge University Press, 2010.

[239] T. J. Osler. Five historical formulas for Pi. *Math. Comp. Educ.*, pages 250–258, 2009.

[240] M. W. Ostrogradsky. De l'integration des fractions rationelles. *Bulletin de la Classe Physico-Mathematiques de l'Academie Imperiale des Sciences de St. Petersbourgh*, IV:145–167, 286–300, 1845.

[241] A. E. Parks. π, e, and other irrational numbers. *Amer. Math. Monthly*, 93:722–723, 1986.

[242] B. Pascal. Sommation des puissances numériques. *Oeuvres complètes*, III:341–367, 1964, *Translation by* A. Knoebel, R. Laudenbacher, J. Lodder, and D. Pengelley, Sums of numerical powers, in *Mathematical Masterpieces: Further Chronicles by the Explorers*, Springer-Verlag, 2007, 32-37.

[243] P. Paule and V. Pillwein. Automatic improvements of Wallis' inequality. In T. Ida et al., editors, *SYNASC 2010, 12th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing*, pages 12–16. IEEE Computer Society, 2011.

[244] P. Paule and A. Riese. A Mathematica q-analogue of Zeilberger's algorithm based on an algebraically motivated approach to q-hypergeometric telescoping. In M. E. H. Ismail and M. Rahman, editors, *Special Functions, q-Series and Related Topics*, volume 14 of *Fields Inst. Comm.*, pages 179–210. Amer. Math. Soc., 1997.

[245] K. A. Penson and J.-M. Sixdeniers. Integral representations of Catalan and related numbers. *Journal of Integer Sequences*, 4: Article 01.2.5, 2001.

[246] M. A. Perlstadt. Some recurrences for sums of powers of binomial coefficients. *J. Number Theory*, 27:304–309, 1987.

[247] M. Petkovsek, H. Wilf, and D. Zeilberger. *A=B*. A. K. Peters, Ltd., 1st edition, 1996.

[248] N. Pippenger. An infinite product for e. *Amer. Math. Monthly*, 87:391, 1980.

[249] A. S. Posamentier and I. Lehman. *The fabulous Fibonacci numbers.* Prometheous Books, 2007.

[250] A. P. Prudnikov, Yu. A. Brychkov, and O. I. Marichev. *Integrals and Series.* Gordon and Breach Science Publishers, 1992.

[251] P. Ribenboim. *Fermat's Last Theorem for Amateurs.* Springer-Verlag, New York, 1st edition, 1999.

[252] J. Riordan. A note on Catalan parentheses. *Amer. Math. Monthly*, 80:904–906, 1976.

[253] J. Riordan. *An Introduction to Combinatorial Analysis.* Dover Publications, New York, 2002.

[254] T. Rivoal. La fonction zeta de Riemann prend une infinité de valeurs irrationnelles aux entiers impairs. *C. R. Acad. Sci. Paris*, 331:267–270, 2000.

[255] J. Roberts. *Elementary Number Theory. A Problem Oriented Approach.* The MIT Press, Cambridge, Massachusetts, 1977.

[256] K. Rosen. *Discrete Mathematics and Its Applications.* McGraw-Hill, 5th edition, 2003.

[257] K. Rosen. *Elementary Number Theory and Its Applications.* Addison Wesley, Reading, Massachusetts, 6th edition, 2010.

[258] M. I. Rosen. A proof of the Lucas-Lehmer test. *Amer. Math. Monthly*, 95:855–856, 1988.

[259] M. Rothstein. *Aspects of symbolic integration and simplification of exponential and primitive functions.* Ph.D. Thesis, Univ. Wisconsin, Madison, 1976.

[260] M. Rothstein. A new algorithm for the integration of exponential and logarithmic functions. *Proc. of the* 1977 *MACSYMA Users Conference, NASA Pub., CP-2012*, pages 263–274, 1977.

[261] M. Rothstein and B. F. Caviness. A structure theorem for exponential and primitive functions. *SIAM J. Comp.*, 8:357–367, 1979.

[262] G. Rzadkowski. A short proof of the explicit formula for Bernoulli numbers. *Amer. Math. Monthly*, 111:432–434, 2004.

[263] G. Rzadkowski. A calculus-based approach to the von Staudt-Clausen theorem. *Math. Gaz.*, 94:308–312, 2010.

[264] Y. Sagher. Counting the rationals. *Amer. Math. Monthly*, 96:823, 1989.

[265] J. Sandor. On certain bounds for the number e, II. *Octogon Math. Mag.*, 11:241–243, 2003.

[266] J. Sandor. On certain bounds for the sequence $(1+1/n)^{n+a}$. *Octogon Math. Mag.*, 13:906–907, 2005.

[267] A. Sarkar. The sum of arctangents of reciprocal squares. *Amer. Math. Monthly*, 98:652–653, 1990.

[268] J. Schrek. *Algebra: A computational approach.* Chapman and Hall, 1st edition, 2000.

[269] H. J. Seifert and P. S. Bruckman. A Fibonacc-ious integral. *Fib. Quart.*, 29:285–287, 1991.

[270] J. Shallit and D. Ross. A simple proof that φ is irrational. *Fib. Quart.*, 13:32,198, 1975.

[271] N. Shar. Bijective proofs of Vajda's ninetieth Fibonacci number identity and related identities. *INTEGERS*, 12:A5: 1–10, 2012.

[272] Zhang Shu and Jia-Yan Yao. Analytic functions over $\mathbb{Z}_p$ and p-regular sequences. *C. R. Acad. Sci. Paris*, 349:947–952, 2011.

[273] J. Shurman. *Geometry of the Quintic.* John Wiley and Sons, Inc., 1997.

[274] J. H. Silverman. *A Friendly Introduction to Number Theory.* Prentice Hall, New Jersey, 2nd edition, 2001.

[275] J. Sondow. A geometric proof that e is irrational and a new measure of its irrationality. *Amer. Math. Monthly*, 113:637–641, 2006.

[276] J. Sondow and H. Yi. New Wallis- and Catalan-type infinite products for π, e, and $\sqrt{2+\sqrt{2}}$. *Amer. Math. Monthly*, 117:912–917, 2010.

[277] M. Spivak. *Calculus*. Publish or Perish Inc., 2nd edition, 1980.

[278] R. Stanley. Log-concave and unimodal sequences in algebra, combinatorics and geometry. Graph theory and its applications: East and West (Jinan, 1986). *Ann. New York Acad. Sci.*, 576:500–535, 1989.

[279] R. Stanley. *Enumerative Combinatorics*, volume 1. Cambridge University Press, 1999.

[280] R. Stanley. *Enumerative Combinatorics*, volume 1. Cambridge University Press, 2nd edition, 2012.

[281] J. Stewart. *Calculus*. Brooks Cole, 7th edition, 2011.

[282] J. Stopple. *A Primer of Analytic Number Theory. From Riemann to Pythagoras*. Cambridge University Press, 2003.

[283] A. Straub, V. Moll, and T. Amdeberhan. The p-adic valuation of k-central binomial coefficients. *Acta Arith.*, 149:31–42, 2009.

[284] N. Strauss, J. Shallit, and D. Zagier. Problem 6625. Some strange 3-adic identities. *Amer. Math. Monthly*, 99:66–69, 1992.

[285] K. R. Stromberg. *An Introduction to Classical Real Analysis*. Wadsworth and Brooks/Cole Advanced Books and Software, Pacific Grove, California, 1981.

[286] X. Sun and V. Moll. The p-adic valuation of sequences counting alternating sign matrices. *Journal of Integer Sequences*, 12:1–21, 2009.

[287] X. Sun and V. Moll. A binary tree representation for the 2-adic valuation of a sequence arising from a rational integral. *Integers*, 10:211–222, 2010.

[288] R. Tauraso. More congruences for central binomial coefficients. *Jour. Number Theory*, 130:2639–2649, 2010.

[289] N. M. Temme. *Special Functions. An Introduction to the Classical Functions of Mathematical Physics*. John Wiley and Sons, New York, 1996.

[290] F. Terkelsen. The fundamental theorem of algebra. *Amer. Math. Monthly*, 83:647, 1976.

[291] J. P. Tignol. *Galois' Theory of Algebraic Equations*. World Scientific Publishing Co. Pte. Ltd, Singapore, 2nd edition, 2002.

[292] J. Touchard. Sur certaines equations fonctionnelles. In *Proc. Inter. Math. Congress, Toronto*, volume I, pages 465–472, 1928.

[293] B. M. Trager. Algebraic factoring and rational function integration. *Proc. EUROSAM'76*, pages 219–226, 1976.

[294] B. M. Trager. *Integration of algebraic functions*. MIT Thesis, Cambridge, Massachusets, 1984.

[295] D. Uminsky and K. Yeats. Unbounded regions of infinitely logconcave sequences. *Elec. Jour. Comb.*, 14:#R72, 2007.

[296] A. van der Poorten. A proof that Euler missed. *Math. Intelligencer*, 1:195–203, 1979.

[297] K. Venkatachaliengar. Elementary proofs of the infinite product for $\sin z$ and allied formulae. *Amer. Math. Monthly*, 69:541–545, 1962.

[298] F. Vieta. Variorum de Rebus Mathematicis Responsorum Liber VII, 1593. In *Opera Omnia, Reprinted*, volume I, pages 398–400 and 436–446. Georg Olms Verlag, Hildesheim, 1593, reprinted 1970.

[299] N. Ja. Vilenkin. *Special Functions and the Theory of Group Representations.* Amer. Math. Soc., Providence, 1968.

[300] J. Villa-Morales. Math Bite: $\mathbb{Q}$ is not complete. *Math. Magazine*, 82:293–294, 2009.

[301] N. N. Vorob′ev. *Fibonacci numbers.* Dover Publications, 2011.

[302] D. D. Wall. Fibonacci series modulo *m*. *Amer. Math. Monthly*, 67:525–532, 1960.

[303] W. Walter. Old and new approaches to Euler's trigonometric formulas. *Amer. Math. Monthly*, 89:225–230, 1982.

[304] Yi Wang and Yeong-Nan Yeh. Proof of a conjecture on unimodality. *Europ. Journal of Comb.*, 26:617–627, 2005.

[305] E. Waring. *Meditationes Algebraicae.* Cambridge University Press, 1770.

[306] J. Wästlund. An elementary proof of the Wallis product formula for pi. *Amer. Math. Monthly*, 114:914–917, 2007.

[307] G. N. Watson. The marquis and the land-agent. *Math. Gazette*, 17:5–17, 1933.

[308] K. Wegschaider. *Computer generated proofs of binomial multi-sum identities.* Master Thesis, RISC-Linz, May 1997.

[309] E. W. Weisstein. Pi continued fraction. From MathWorld–A Wolfram Web resource.

[310] M. Werman and D. Zeilberger. A bijective proof of Cassini's Fibonacci identity. *Disc. Math.*, 58:109, 1986.

[311] E. T. Whittaker and G. N. Watson. *Modern Analysis.* Cambridge University Press, 1962.

[312] A. J. Wiles. Modular elliptic curves and Fermat's Last Theorem. *Ann. Math.*, 142:443–551, 1995.

[313] H. S. Wilf. *generatingfunctionology.* Academic Press, 1st edition, 1990.

[314] J. Wolstenholme. On certain properties of prime numbers. *Quart. J. Math.*, 5:35–39, 1862.

[315] Z. Yachas. The simplest proof that PHI is irrational. *The Personal Journal of Shalosh B Ekhad.*

[316] J. Yuan, Z. Lu, and A. L. Schmidt. On recurrences for sums of powers of binomial coefficients. *Jour. Number Theory*, 128:2784–2794, 2008.

[317] D. Zagier. A one-sentence proof that every prime $p \equiv 1 \bmod 4$ is a sum of two squares. *Amer. Math. Monthly*, 97:144, 1990.

[318] D. Zagier. Newman's short proof of the Prime Number Theorem. *Amer. Math. Monthly*, 104:705–708, 1997.

[319] D. Zagier. A modified Bernoulli number. *Nieuw Archief voor Wiskunde*, 16:63–72, 1998.

[320] D. Zeilberger. Theorems for a price: Tommorow's semi-rigorous mathematical culture. *Notices AMS*, 40:978–981, 1993.

[321] D. Zeilberger. Proof of the alternating sign matrix conjecture. *Elec. Jour. Comb.*, 3:1–78, 1996.

[322] D. Zeilberger. The holonomic ansatz II: Automatic discovery (!) and proof (!!) of holonomic determinant evaluations. *Ann. Comb.*, 11:241–247, 2007.

[323] W. Zudilin. One of the numbers $\zeta(5)$, $\zeta(7)$, $\zeta(9)$, $\zeta(11)$ is irrational. *Russian Math. Surveys*, 56:774–776, 2001.

[324] W. Zudilin. Apéry's theorem. Thirty years after. (An elementary proof of Apéry's theorem.) *Int. J. Math. Comput. Sci.*, 4:9–19, 2009.

Index

New mathematics often comes about by probing what is already known. Mathematicians will change the parameters in a familiar calculation or explore the essential ingredients of a classic proof. Almost magically, new ideas emerge from this process. This book examines elementary functions, such as those encountered in calculus courses, from this point of view of experimental mathematics. The focus is on exploring the connections between these functions and topics in number theory and combinatorics. There is also an emphasis throughout the book on how current mathematical software can be used to discover and prove interesting properties of these functions.

The book provides a transition between elementary mathematics and more advanced topics, trying to make this transition as smooth as possible. Many topics occur in the book, but they are all part of a bigger picture of mathematics. By delving into a variety of them, the reader will develop this broad view. The large collection of problems is an essential part of the book. The problems vary from routine verifications of facts used in the text to the exploration of open questions.

ISBN 978-0-8218-8795-0

9 780821 887950

STML/65

For additional information
and updates on this book, visit
www.ams.org/bookpages/stml-65

AMS *on the* Web
www.ams.org