DORIN ANDRICA OVIDIU BAGDASAR GEORGE-CĂTĂLIN ȚURCAȘ

TOPICS ON DISCRETE MATHEMATICS AND COMBINATORICS

SECOND EDITION

$$\Phi_n(z) = \prod_{d|n} \left(z^d - 1\right)^{\mu(n/d)}$$

PRESA UNIVERSITARĂ CLUJEANĂ

Dorin Andrica | Ovidiu Bagdasar | George-Cătălin Țurcaș

TOPICS ON DISCRETE MATHEMATICS AND COMBINATORICS

Dorin Andrica | Ovidiu Bagdasar | George-Cătălin Țurcaș

TOPICS
ON DISCRETE MATHEMATICS AND COMBINATORICS

SECOND EDITION

PRESA UNIVERSITARĂ CLUJEANĂ / CLUJ UNIVERSITY PRESS
2024

Referenți științifici:

Prof. univ. dr. Andrei Mărcuș

Conf. univ. dr. Cornel-Sebastian Pintea

ISBN 978-606-37-2482-4

Universitatea Babeş-Bolyai
Presa Universitară Clujeană
Director: Codruța Săcelean
Str. Hasdeu nr. 51
400371 Cluj-Napoca, România
Tel./fax: (+40)-264-597.401
E-mail: editura@ubbcluj.ro
http://www.editura.ubbcluj.ro/

Preface

The book presents modern results in discrete mathematics and combinatorics, its purpose being to popularise recent developments in this area, and to encourage further research. Structured in ten chapters, it provides theoretical results illustrated by many examples and applications.

The first part of the book is dedicated to useful identities for polynomials, sums and products, along with methods of proof and counting strategies.

- Chapter 1 presents fundamental identities and techniques required for efficient work with quadratics and polynomials of higher degree.
- Chapter 2 is dedicated to important examples of sums and products, including telescopic sums, sums of perfect powers, trigonometric sums and finite products.
- Chapter 3 presents fundamental proof techniques, including proof by contradiction, induction, or by the pigeon hole principle.
- Chapter 4 is devoted to counting strategies. Here we review permutations, combinations, binomial coefficients. We present numerous results for classical sets and also for multisets. We then illustration the inclusion-exclusion principle, and counting strategies focused on bijections, or multiple ways of counting, as well as by using Hall's marriage theorem.

The second presents key results regarding generating functions and recursive processes, with an emphasis on recent work on sequences of Lucas and Pell-Lucas polynomials, and integral representations for classical sequences.

- In Chapter 5 we discuss the general theory of ordinary and exponential generating functions, supported by numerous examples. In this context we also present a useful versions of the Cauchy integral formula, which has many applications.
- Chapter 6 is dedicated to recursive processes, with separate sections for first, second, and higher-order linear recursions. We then discuss the sequences of Lucas and Pell-Lucas polynomials, for which we provide ordinary and exponential generating functions, as well as explicit formulae for Fibonacci, Lucas, Pell and Pell-Lucas polynomials. In particular, we discuss applications to classical sequences, for which we also provide some integral representations.

The third part of the book is devoted to special polynomials, starting with polynomials in multiple variables, followed by cyclotomic and inverse cyclotomic polynomials.

- Chapter 7 presents key results on symmetric polynomials, presenting Newton's formulas, along side number theoretic applications.
- Chaper 8 is devoted to cyclotomic polynomials and their numerous applications. We start with some background information on arithmetic functions, Möbius function and Ramanujan sums. We then discuss the definition and basic properties of the cyclotomic polynomials, along with results on the magnitude (Suzuki), integral formula, or various recent recurrent formulae for the coefficients of cyclotomic polynomials, some of which are original. In a similar framework we also analyse the inverse cyclotomic polynomials, whose investigation is more recent.
- Chapter 9 presents a variety of special polynomials, including polygonal, Gaussian, multinomial, Catalan polynomials, for which we discuss recursive and integral formulae for the coefficients, related integer sequences, and combinatorial interpretations. Much of this work involves original research results published by the authors in the recent years.

Finally, Chapter 10 is devoted to the study of special types of ordered partitions of sets of multisets. We start from the classical signum equations, and then build the theory allowing us to study k-partitions with equal sums of multisets, whose number is computed using integral formulae. The results are linked to diophantine equations and novel integer sequences.

The book comes with **244** references suggesting further reading, and an index to help the readers to easily navigate the contents. It can be a useful resource for researchers and scholars interested in recent advances in the field of discrete mathematics, postgraduate students in college or university and their instructors, or advanced high school students.

We would like to thank Professor Andrei Mărcuş and Associate Professor Cornel Pintea for their constructive remarks and suggestions, which helped us improve the quality of the manuscript. We also thank them for recommending this book for publication.

Special thanks to our families for their continuous and discrete support.

The authors
February 2023

Preface to the Second Edition

This Second Edition of the book is motivated by the significant number of results published over the last two years, concerning the coefficients of the cyclotomic and inverse cyclotomic polynomials, for which we have found new integral and recursive formulae involving Ramanujan sums [23, 24], upper bounds of coefficients [29], and closed formulae and properties of the coefficients of ternary cyclotomic and inverse cyclotomic polynomials [30]. Other authors have also extended and applied our work [131, 265].

Chapters from the first edition of this book were used for and discussed in a course on Discrete Mathematics at Babes-Bolyai University. This experience has allowed us to incorporate new problems and discussions that arose during lectures and seminars into this revised edition. These additions aim to enrich the reader's understanding by addressing practical questions and enhancing theoretical insights. Several minor typos were also detected and corrected during these interactive sessions.

Furthermore, Chapter 3 has been expanded with illustrative examples related to the pigeonhole principle and mathematical induction, linked to the solution of some recent Olympiad problems. Additionally, a new section dedicated to Erdős-Surányi sequences has been added, broadening the scope of topics covered.

Finally, we have included recent citations and applications of the results presented in this book, and updated the bibliography.

The authors
December 2024

Contents

Chapter 1
Identities. Polynomials

1.1 Basic identities

We start by exploring various polynomial identities that are commonly used in mathematics and emphasize some of their practical applications. Identities are an essential tool in solving many mathematical problems, ranging from problems in algebra to geometry and beyond. They frequently allow one to simplify expressions and evaluate complicated functions.

1. Difference of powers.

$$a^n - b^n = (a-b)(a^{n-1}b^0 + a^{n-2}b^1 + \cdots + a^1 b^{n-2} + b^{n-1}a^0).$$

Some useful forms of this identity occur for $n = 2$ where we have

$$a^2 - b^2 = (a-b)(a+b),$$

and for $n = 3$ in which case

$$a^3 - b^3 = (a-b)(a^2 + ab + b^2).$$

Note that when $a = 1$ one obtains the sum of a geometric series

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

2. Sum of odd powers.

$$a^{2n+1} + b^{2n+1} = (a+b)(a^{2n}b^0 - a^{2n-1}b^1 + \cdots - a^1 b^{2n-1} + b^{2n}a^0).$$

This identity follows by substituting $b' = -b$ into identity 1. The most common form is obtained for $n = 1$, giving the sum of cubes:

$$a^3 + b^3 = (a+b)(a^2 - ab + b^2).$$

Also, when $a = 1$, one obtains the sum of an alternate geometric series:

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

3. Product of sums of powers.

$$(x + a)(x^2 + a^2)\cdots(x^{2^{n-1}} + a^{2^{n-1}}) = \frac{x^{2^n} - a^{2^n}}{x - a}. \tag{1.1}$$

The proof to this identity follows by multiplication of both sides by $x - a$ and by successive application of the difference of squares formula

$$(u - v)(u + v) = u^2 - v^2.$$

After $n - 1$ steps we get

$$(x^{2^{n-1}} - a^{2^{n-1}})(x^{2^{n-1}} + a^{2^{n-1}}) = x^{2^n} - a^{2^n},$$

and this relation is obvious since

$$x^{2^n} - a^{2^n} = (x^{2^{n-1}})^2 - (a^{2^{n-1}})^2.$$

4. Collapsing trinomial factorization.

$$(x^2 - ax + a^2)\cdots(x^{2^n} - x^{2^{n-1}}a^{2^{n-1}} + a^{2^n}) = \frac{x^{2^{n+1}} + x^{2^n}a^{2^n} + a^{2^{n+1}}}{x^2 + ax + a^2}.$$

The idea of proof is similar to the proof given for the previous identity. Multiply both sides by $x^2 + ax + a^2$ and use successively the relation

$$(u^2 + uv + v^2)(u^2 - uv + v^2) = (u^2 + v^2)^2 - (uv)^2 = u^4 + u^2v^2 + v^4.$$

After n steps we get

$$(x^{2^n} + x^{2^{n-1}}a^{2^{n-1}} + a^{2^n})(x^{2^n} - x^{2^{n-1}}a^{2^{n-1}} + a^{2^n}) = x^{2^{n+1}} + x^{2^n}a^{2^n} + a^{2^{n+1}},$$

and the last relation is true because the same argument.

Example 1.1. *Let n be a positive integer. Prove the identity*

$$2^{4n+2} + 1 = (2^{2n+1} + 2^{n+1} + 1)(2^{2n+1} - 2^{n+1} + 1).$$

Solution. We have

$$(2^{2n+1} + 2^{n+1} + 1)(2^{2n+1} - 2^{n+1} + 1) = (2^{2n+1} + 1)^2 - (2^{n+1})^2$$

$$= 2^{4n+2} + 2^{2n+2} + 1 - 2^{2n+2} = 2^{4n+2} + 1.$$

Example 1.2 (Balkan 1997). *Let x,y be non-zero real numbers with $|x| \neq |y|$ and*

$$\frac{x^2+y^2}{x^2-y^2} + \frac{x^2-y^2}{x^2+y^2} = k,$$

for some real number k. Find in terms of k the value of

$$\frac{x^8+y^8}{x^8-y^8} + \frac{x^8-y^8}{x^8+y^8}.$$

Solution. The equality

$$\frac{x^2+y^2}{x^2-y^2} + \frac{x^2-y^2}{x^2+y^2} = k$$

implies

$$\frac{(x^2+y^2)^2+(x^2-y^2)^2}{x^4-y^4} = k,$$

hence

$$\frac{x^4+y^4}{x^4-y^4} = \frac{k}{2'}$$

from where one obtains $\left(\frac{x}{y}\right)^2 = \frac{k+2}{k-2}$. Therefore

$$\begin{aligned}\frac{x^8+y^8}{x^8-y^8} + \frac{x^8-y^8}{x^8+y^8} &= \frac{(x^8+y^8)^2+(x^8-y^8)^2}{x^{16}-y^{16}} = \frac{2(x^{16}+y^{16})}{x^{16}-y^{16}} \\ &= 2\frac{\left(\frac{k+2}{k-2}\right)^4+1}{\left(\frac{k+2}{k-2}\right)^4-1} = 2\frac{(k+2)^4+(k-2)^4}{(k+2)^4-(k-2)^4}.\end{aligned}$$

Example 1.3. *Find a relation between the numbers a,b,c if*

$$x+\frac{1}{x} = a, \quad y+\frac{1}{y} = b, \quad xy+\frac{1}{xy} = c.$$

Solution. We have

$$\left(x+\frac{1}{x}\right)\left(y+\frac{1}{y}\right) = xy+\frac{1}{xy}+\frac{x}{y}+\frac{y}{x},$$

hence

$$\frac{x}{y}+\frac{y}{x} = ab-c.$$

On the other hand

$$\left(\frac{x}{y}+\frac{y}{x}\right)\left(xy+\frac{1}{xy}\right)=x^2+y^2+\frac{1}{x^2}+\frac{1}{y^2}$$

$$=\left(x+\frac{1}{x}\right)^2+\left(y+\frac{1}{y}\right)^2-4=a^2+b^2-4,$$

hence

$$(ab-c)c=a^2+b^2-4.$$

The desired relation is

$$a^2+b^2+c^2-abc=4.$$

Example 1.4 (Balkan 2000). *Let x,y be integers such that*

$$x^3+y^3+(x+y)^3+30xy=2000.$$

Prove that $x+y=10$.

Solution. We have

$$\begin{aligned}E&=x^3+y^3+(x+y)^3+30xy-2000\\&=2(x+y)^3-3x^2y-3xy^2+30xy-2000\\&=2[(x+y)^3-1000]-3xy(x+y-10)\\&=(x+y-10)[2((x+y)^2+10(x+y)+100)-3xy]\\&=(x+y-10)(2x^2+xy+2y^2+20x+20y+200)\\&=(x+y-10)F.\end{aligned}$$

Since

$$\begin{aligned}F&=2x^2+xy+2y^2+20x+20y+200\\&=(x^2+xy+y^2)+(x^2+20x+100)+(y^2+20y+100)\\&=\frac{x^2+y^2+(x+y)^2}{2}+(x+10)^2+(y+10)^2>0,\end{aligned}$$

it follows that $x+y=10$.

Example 1.5. *Let $f_n=2^{2^n}+1$, $n=0,1,\ldots$, be the Fermat's numbers. Prove that*

$$f_n=f_0f_1f_2\cdots f_{n-1}+2.$$

Solution 1. By formula (1.1) (product of sum of powers) for $a=1$ to get

$$(x+1)(x^2+1)(x^4+1)\ldots(x^{2^{n-1}}+1)=\frac{x^{2^n}-1}{x-1}.$$

Taking $x = 2$ one obtains $f_0 \cdot f_1 \cdot f_2 \dots f_{n-1} = 2^{2^n} - 1$, hence if follows that $f_n = f_0 \cdot f_1 \cdot f_2 \dots f_{n-1} + 2$, and we are done.

Solution 2. We have

$$f_k = 2^{2^k} + 1 = 2^{2^{k-1} \cdot 2} + 1 = (f_{k-1} - 1)^2 + 1 = f_{k-1}^2 - 2f_{k-1} + 2,$$

hence $f_k - 2 = f_{k-1}(f_{k-1} - 2)$. Multiplying for $k = 1, 2, \dots, n$ yields

$$f_n - 2 = f_{n-1} \dots f_1 \cdot f_0(f_0 - 2),$$

and since $f_0 = 3$, we obtain the desired relation.

Example 1.6. *Factorize* $(x + y + z)^3 - x^3 - y^3 - z^3$.

Solution. Let $E = E(x, y, z)$ be the expression to be factorized. Using the difference of cubes and the sum of cubes, we have

$$\begin{aligned} E &= (x + y + z)^3 - x^3 - (y^3 + z^3) \\ &= (y + z)[(x + y + z)^2 + x(x + y + z) + x^2] - (y + z)(y^2 - yz + z^2) \\ &= (y + z)(3x^2 + 3xy + 3yz + 3zx) = 3(x + y)(y + z)(z + x). \end{aligned}$$

Remark. From the above factorization it follows that

$$(x + y + z)^3 = x^3 + y^3 + z^3$$

if and only if $x + y = 0$ or $y + z = 0$, or $z + x = 0$.

Example 1.7. *Let $a \neq 1$ be a complex number and let n be a positive integer. Prove the identity*

$$(1 + a + a^2 + \dots + a^n)(1 + a^{n+1}) = 1 + a + a^2 + \dots + a^{2n+1}.$$

Solution. Just multiply in the left hand side and get

$$(1 + a + a^2 + \dots + a^n) + (a^{n+1} + a^{n+2} + \dots + a^{2n+1}) = 1 + a + \dots + a^{2n+1}.$$

Example 1.8. *Show that if $a, b, c \in \mathbb{C}$ satisfy $abc \neq 0$ and $a + b + c = 0$, then*

$$\frac{1}{-a^2 + b^2 + c^2} + \frac{1}{a^2 - b^2 + c^2} + \frac{1}{a^2 + b^2 - c^2} = 0.$$

Solution. We have $a = -(b + c)$, hence we get

$$-a^2 + b^2 + c^2 = -(b + c)^2 + b^2 + c^2 = -2bc.$$

Similarly,

$$a^2 - b^2 + c^2 = -2ac \quad \text{and} \quad a^2 + b^2 - c^2 = -2ab.$$

Therefore,

$$\frac{1}{-a^2+b^2+c^2}+\frac{1}{a^2-b^2+c^2}+\frac{1}{a^2+b^2-c^2}=-\frac{1}{2}\left(\frac{1}{bc}+\frac{1}{ac}+\frac{1}{ab}\right)$$

$$=-\frac{1}{2abc}(a+b+c)=0.$$

Example 1.9. *Let $n\geq 1$ be an integer. Prove that $3^{2^n}-1$ contains in its factorization at least $2n+1$ primes, not necessarily distinct.*

Solution. From identity (1.1) we have

$$\begin{aligned}3^{2^n}-1&=2(3+1)(3^2+1)\cdots(3^{2^{n-1}}+1)\\&=2^3(3^2+1)\cdots(3^{2^{n-1}}+1).\end{aligned}$$

Each factor $3^2+1, 3^{2^2}+1,\ldots,3^{2^{n-1}}+1$ is even, hence it is divisible by 2. We get $3+n-1=n+2$ factors of 2. We also have at least $n-1$ other primes in factorization of $3^{2^n}-1$, and the conclusion follows.

Example 1.10 (Romania 2000). *If x,y,z,t are non-zero real numbers. Determine the sum $x+y+z+t$ if the numbers satisfy*

$$\begin{aligned}x+y+z&=t\\\frac{1}{x}+\frac{1}{y}+\frac{1}{z}&=\frac{1}{t}\\x^3+y^3+z^3&=1000^3.\end{aligned}$$

Solution. Multiplying the first two relations we get

$$(x+y+z)(xy+yz+zx)=xyz,$$

hence

$$(x+y)(y+z)(z+x)=0,$$

from where $x+y=0$, $y+z=0$, or $z+x=0$, that is $x+y+z+t=2t$. From the last equality we get $t=1000$, hence $x+y+z+t=2000$.

1.2 A useful identity

The following factorization occurs in a large number of problems, but owing to its relative obscurity is oftentimes overlooked. It can make a problem much easier! For any complex numbers a,b,c, we have

$$a^3+b^3+c^3-3abc=(a+b+c)(a^2+b^2+c^2-ab-bc-ca). \tag{1.2}$$

Proof 1. Multiply the factors on the right hand and cancel the similar terms.

Proof 2. Let P denote the polynomial with roots a,b,c:

$$P(X) = X^3 - (a+b+c)X^2 + (ab+bc+ca)X - abc.$$

Because a,b,c satisfy the equation $P(x) = 0$, we obtain

$$a^3 - (a+b+c)a^3 + (ab+bc+ca)a - abc = 0,$$

$$b^3 - (a+b+c)b^3 + (ab+bc+ca)b - abc = 0,$$

$$c^3 - (a+b+c)c^3 + (ab+bc+ca)c - abc = 0.$$

Adding up these three equalities yields

$$a^3+b^3+c^3 - (a+b+c)(a^2+b^2+c^2) + (ab+bc+ca)(a+b+c) - 3abc = 0.$$

Hence

$$a^3+b^3+c^3 - 3abc = (a+b+c)(a^2+b^2+c^2-ab-bc-ca).$$

Proof 3. Another way to obtain the identity (1.2) is to use the determinant:

$$D = \begin{vmatrix} a & b & c \\ c & a & b \\ b & c & a \end{vmatrix}.$$

Expanding D, we obtain

$$D = a^3+b^3+c^3-3abc.$$

On the other hand, adding all columns to the first one gives

$$\begin{aligned} D &= \begin{vmatrix} a+b+c & b & c \\ a+b+c & a & b \\ a+b+c & c & a \end{vmatrix} = (a+b+c)\begin{vmatrix} 1 & b & c \\ 1 & a & b \\ 1 & c & a \end{vmatrix} \\ &= (a+b+c)(a^2+b^2+c^2-ab-bc-ca). \end{aligned}$$

Remark. 1° Whenever $a+b+c=0$, we have that

$$a^3+b^3+c^3 = 3abc. \tag{1.3}$$

2° For $a,b,c \in \mathbb{R}$ one has $a^3+b^3+c^3 = 3abc$ if and only if $a+b+c=0$ or $a=b=c$. Indeed, if $a+b+c \neq 0$, then from (1.2) we get

$$a^2+b^2+c^2-ab-bc-ca=0.$$

That is $(a-b)^2+(b-c)^2+(c-a)^2=0$, and the conclusion follows.

3° As we have seen above, the expression

$$a^2+b^2+c^2-ab-bc-ca$$

can also be written as

$$\frac{1}{2}[(a-b)^2+(b-c)^2+(c-a)^2].$$

We obtain another version of the identity (1.2):

$$a^3+b^3+c^3-3abc=\frac{1}{2}(a+b+c)[(a-b)^2+(b-c)^2+(c-a)^2].$$

4° The complete factorization of $a^3+b^3+c^3-3abc$ is

$$a^3+b^3+c^3-3abc=(a+b+c)(a+b\omega+c\omega^2)(a+b\omega+c\omega^2) \qquad (1.4)$$

where ω is a cubic root of unity different from 1. Indeed, let us regard

$$a^2+b^2+c^2-ab-bc-ca$$

as a quadratic in a, with parameters b,c. This quadratic has discriminant

$$\Delta=(b+c)^2-4(b^2+c^2-bc)=-3(b-c)^2.$$

Hence its roots are

$$a_1=\frac{b+c-i(b-c)\sqrt{3}}{2}=b\frac{1-i\sqrt{3}}{2}+c\frac{1+i\sqrt{3}}{2}$$

and

$$a_2=\frac{b+c+i(b-c)\sqrt{3}}{2}=b\frac{1+i\sqrt{3}}{2}+c\frac{1-i\sqrt{3}}{2}.$$

Setting $\omega=\dfrac{-1+i\sqrt{3}}{2}$, one of the primitive cubic roots of the unity, we have

$$\omega^2=\frac{-1-i\sqrt{3}}{2},$$

hence $a_1=-b\omega-c\omega^2$ and $a_2=-b\omega^2-c\omega$. This gives the factorization

$$a^2+b^2+c^2-ab-bc-ca=(a+b\omega+c\omega^2)(a+b\omega^2+c\omega),$$

which leads to the identity (1.4).

Example 1.11. *Factor* $(x+2y-3z)^3+(y+2z-3x)^3+(z+2x-3y)^3$.

Solution. Denote

$$a=x+2y-3z,\quad b=y+2z-3x,\quad c=z+2x-3y,$$

and observe that $a+b+c=0$. By (1.3) it follows

$$a^3+b^3+c^3=3abc,$$

hence the desired factorization is

$$\begin{aligned}&(x+2y-3z)^3+(y+2z-3x)^3+(z+2x-3y)^3\\&=3(x+2y-3z)(y+2z-3x)(z+2x-3y).\end{aligned}$$

Example 1.12. *Let* a,b,c *be integers such that*

$$(a-b)^2+(b-c)^2+(c-a)^2=abc.$$

Prove that $a^3+b^3+c^3$ *is divisible by* $a+b+c+6$.

Solution. We first notice that at least one of a,b,c is even. Indeed, if a,b,c are all odd, the left-hand side of the given equality is even while the right-hand side is odd, a contradiction. Because

$$a^3+b^3+c^3-3abc=(a+b+c)(a^2+b^2+c^2-ab-bc-ca),$$

and

$$a^2+b^2+c^2-ab-bc-ca=\frac{1}{2}[(a-b)^2+(b-c)^2+(c-a)^2]=\frac{abc}{2},$$

we get

$$a^3+b^3+c^3-3abc=(a+b+c)\frac{abc}{2},$$

hence

$$a^3+b^3+c^3=\frac{abc}{2}(a+b+c+6),$$

and since $\dfrac{abc}{2}$ is an integer, the conclusion follows.

Example 1.13. *Prove that*

$$\sqrt[3]{45+29\sqrt{2}}+\sqrt[3]{45-29\sqrt{2}}$$

is a rational number.

Solution. Let $a=\sqrt[3]{45+29\sqrt{2}}+\sqrt[3]{45-29\sqrt{2}}$. Because

$$a-\sqrt[3]{45+29\sqrt{2}}-\sqrt[3]{45-29\sqrt{2}}=0,$$

we have

$$a^3-(45+29\sqrt{2})-(45-29\sqrt{2})=3a\sqrt[3]{(45+29\sqrt{2})(45-29\sqrt{2})},$$

which is equivalent to

$$a^3-21a-90=0$$

or

$$(a-6)(a^2+6a+15)=0.$$

The equation $a^2+6a+15=0$ has no real roots; hence

$$\sqrt[3]{45+29\sqrt{2}}+\sqrt[3]{45-29\sqrt{2}}=6,$$

a rational number.

Example 1.14. *Let r be a real number such that*

$$\sqrt[3]{r}+\frac{1}{\sqrt[3]{r}}=3.$$

Determine the value of $r^9+\dfrac{1}{r^9}$.

Solution. From $\sqrt[3]{r}+\dfrac{1}{\sqrt[3]{r}}-3=0$, we obtain

$$r+\frac{1}{r}-27=3\sqrt[3]{r}\frac{1}{\sqrt[3]{r}}(-3)=-9,$$

which gives $r+\dfrac{1}{r}=18$. Now, from $r+\dfrac{1}{r}-18=0$, it follows that

$$r^3+\frac{1}{r^3}-18^3=3r\frac{1}{r}(-18)=-3\cdot 18,$$

hence

$$r+\frac{1}{r^3}=18^3-3\cdot 18.$$

Again, from $r^3+\dfrac{1}{r^3}-(18^3-3\cdot 18)=0$, we get

$$r^9-\frac{1}{r^9}-(18^3-3\cdot 18)^3=-3(18^3-3\cdot 18),$$

therefore

$$r^9+\frac{1}{r^9}=(18^3-3\cdot 18)^3-3(18^3-3\cdot 18).$$

Example 1.15. *Let a,b, and c be the side lengths of a triangle. Prove that*

$$\sqrt[3]{\frac{a^3+b^3+c^3+3abc}{2}} \geq \max\{a,b,c\}.$$

Solution. Assume, with no loss of generality, that $a \geq b \geq c$. We have to prove that

$$\sqrt[3]{\frac{a^3+b^3+c^3+3abc}{2}} \geq a,$$

which is equivalent to

$$-a^3+b^3+c^3+3abc \geq 0.$$

Since

$$-a^3+b^3+c^3+3abc = (-a)^3+b^3+c^3-3(-a)bc,$$

the latter expression factors into

$$\frac{1}{2}(-a+b+c)((a+b)^2+(a+c)^2+(b-c)^2).$$

The conclusion follows by the triangle inequality $b+c>a$.

Example 1.16. *Factorize* $(x-y)^3+(y-z)^3+(z-x)^3$.

Solution. Observe that if $a+b+c=0$, then it follows from (1.2) that

$$a^3+b^3+c^3 = 3abc.$$

Because

$$(x-y)+(y-z)+(z-x)=0,$$

we obtain the factorization

$$(x-y)^3+(y-z)^3+(z-x)^3 = 3(x-y)(y-z)(z-x).$$

Example 1.17. *Prove the arithmetic-geometric mean inequality for three nonnegative real numbers x,y,z.*

Solution. We will show that

$$\frac{x+y+z}{3} \geq \sqrt[3]{xyz},$$

with equality for $x=y=z$. Setting $x=a^3$, $y=b^3$, $z=c^3$, we have

$$x+y+z-3\sqrt[3]{xyz} = a^3+b^3+c^3-3abc$$
$$= \frac{1}{2}(a+b+c)[(a-b)^2+(b-c)^2+(c-a)^2].$$

As the right-hand side is nonnegative, we must have $a+b+c \geq 3\sqrt[3]{abc}$ as desired. Furthermore, equality occurs only when the right-hand side of our relation is zero, namely, when $x=y=z$, which is equivalent to $a=b=c$.

Example 1.18. *Show that* $\sqrt[3]{2+\sqrt{5}}+\sqrt[3]{2-\sqrt{5}}$ *is a rational number.*

Solution. Set $x=\sqrt[3]{2+\sqrt{5}}$, $y=\sqrt[3]{2-\sqrt{5}}$, $z=-1$. Then we have

$$x^3+y^3+z^3-3xyz = 2+\sqrt{5}+2-\sqrt{5}-1-3(-1)\sqrt[3]{-1} = 0.$$

Hence

$$(x+y+z)[(x-y)^2+(y-z)^2+(z-x)^2] = 0.$$

As $x \neq y \neq z$, we must have

$$(x-y)^2+(y-z)^2+(z-x)^2 > 0.$$

Hence $x+y+z=0$, $x+y=1$ as desired.

Example 1.19. *If* $a,b,c \in \mathbb{Z}$ *satisfy* $a+b\sqrt[3]{2}+c\sqrt[3]{4}=0$, *then* $a=b=c=0$.

Solution. Set $x=a$, $y=b\sqrt[3]{2}$, $z=\sqrt[3]{4}$. Then we obtain

$$x^3+y^3+z^3-3xyz = (x+y+z)(x^2+y^2+z^2-xy-yz-zx) = 0.$$

Hence we have

$$a^3+2b^3+4c^3 = 6abc.$$

Suppose that a',b',c' are not all zero. Without loss of generality, suppose that a,b,c are relatively prime. Taking our relation modulo 2, we find that $a^3 \equiv 0 \pmod 2$. Hence $a=2a'$ for some integer a'. Then we have

$$8a'^3+2b^3+4c^3 = 12a'bc.$$

Dividing through by 2, we get

$$4a'^3+b^3+2c^3 = 6a'bc.$$

Working modulo 2, we find that $b=2b'$ for an integer b', hence we may write

$$4a'^3+8b'^3+2c^3 = 12a'b'c.$$

Dividing through by 2, we get

$$2a'^3 + 4b'^3 + c^3 = 6a'b'c.$$

Working modulo 2 a third time, we find that $c = 2c'$ for some integer c'. Hence all of a, b, c are divisible by 2, contradicting our earlier assumption. It follows that $a = b = c = 0$, which ends the proof.

Example 1.20. *Show that there exists a unique equilateral triangle with vertices on the graph of the equation*

$$x^3 + 3xy + y^3 = 1.$$

Find the area of this triangle.

Solution. Set $z = -1$. Then we have

$$x^3 + y^3 + z^3 - 3xyz = 0.$$

Hence either

$$x + y + z = 0 \quad \text{or} \quad (x-y)^2 + (y-z)^2 + (z-x)^2 = 0.$$

In the former case, we have $x + y = 1$. In the latter case, we have $x = y = -1$. Hence the graph of this equation consists of one line and a point not on that line. Hence any equilateral triangle with vertices among the points of the graph mush have one vertex at $(-1,-1)$, and altitude from this vertex to the point $(1/2,1/2)$. Then in this case such an equilateral triangle must be uniquely determined, and have area

$$(3\sqrt{2}/2)^2/\sqrt{3} = 3\sqrt{3}/2.$$

1.3 Working with quadratic polynomials

A **quadratic polynomial** is any polynomial of the form

$$f = ax^2 + bx + c, \tag{1.5}$$

with a, b, c complex numbers, with a nonzero. The most important theoretical results regarding the quadratic polynomials are the following.

The **zeros** of f are the roots of the quadratic equation

$$ax^2 + bx + c = 0. \tag{1.6}$$

If $\Delta = b^2 - 4ac$ is its discriminant, then the zeros of f are given by

$$x_1 = \frac{-b + \sqrt{\Delta}}{2a}, \quad x_2 = \frac{-b - \sqrt{\Delta}}{2a}. \tag{1.7}$$

If $\Delta = 0$, then the quadratic equation (1.6) has one double root

$$x_1 = x_2 = -\frac{b}{2a}.$$

From (1.7), we easily can deduce the formulas

$$x_1 + x_2 = -\frac{b}{a}, \quad x_1 x_2 = \frac{c}{a},$$

called **Viete's relations**. Further, we have the factorization

$$f = a(x - x_1)(x - x_2). \tag{1.8}$$

Example 1.21. *Factorize* $b^4 - 2ab^2 + a^2 - b^2 + 2b - 1$.

Solution. Looking at $E(a,b) = b^4 - 2ab^2 + a^2 - b^2 + 2b - 1$ as to a quadratic polynomial in a, we have

$$E(a,b) = a^2 - 2b^2 a + b^4 - b^2 + 2b - 1.$$

The discriminant of equation $E(a,b) = 0$ is

$$\Delta = 4b^4 - 4(b^4 - b^2 + 2b - 1) = 4(b^2 - 2b + 1) = [2(b-1)]^2.$$

The roots of $E(a,b) = 0$ are $a_1 = b^2 + b - 1$ and $a_2 = b^2 - b + 1$, and it follows

$$E(a,b) = (a - b^2 - b + 1)(a - b^2 + b - 1) = (b^2 + b - a - 1)(b^2 - b - a + 1).$$

Remark. To factorize $E(a,b)$ in linear factor on b over $\mathbb{C}$, we can write

$$\begin{aligned} b^2 + b - a - 1 &= \left(b + \frac{1}{2}\right)^2 - \left(a + \frac{5}{4}\right) \\ &= \left(b + \frac{1}{2} + \sqrt{a + \frac{5}{4}}\right)\left(b + \frac{1}{2} - \sqrt{a + \frac{5}{4}}\right) \\ b^2 - b - a + 1 &= \left(b - \frac{1}{2}\right)^2 - \left(a - \frac{3}{4}\right) \\ &= \left(b - \frac{1}{2} + \sqrt{a - \frac{3}{4}}\right)\left(b - \frac{1}{2} - \sqrt{a - \frac{3}{4}}\right). \end{aligned}$$

Example 1.22. *Write the polynomial*

$$P(x) = ax^4 + bx^3 + cx^2 + dx + e$$

as a product of two quadratic polynomials, if $a + d = b + e = c$.

Solution. We can write

$$\begin{aligned} P(x) &= ax^4 + bx^3 + cx^2 + (c-a)x + c - b \\ &= ax^4 - ax + bx^3 - b + cx^2 + cx + c \\ &= ax(x^3-1) + b(x^3-1) + c(x^2+x+1) \\ &= (x^2+x+1)[ax(x-1) + b(x-1) + c] \\ &= (x^2+x+1)[ax^2 + (b-a)x + c - b]. \end{aligned}$$

Example 1.23. *Solve the equation*

$$x^4 - (2m+1)x^3 + (m-1)x^2 + (2m^2+1)x + m = 0,$$

where m is a real parameter.

Solution. For $m = 0$ the equation becomes

$$x^4 - x^3 - x^2 + x = 0$$

and has roots $x_1 = 0$, $x_2 = -1$, $x_3 = x_4 = 1$.

If $m \neq 0$, we will solve the equation in terms of m. We have

$$2xm^2 + (x^2 - 2x^3 + 1)m + x^4 - x^3 - x^2 + x = 0$$

and

$$\Delta = (x^2 - 2x^3 + 1)^2 - 8x^2(x^3 - x^2 - x + 1) = (2x^3 - 3x^2 + 1)^2.$$

It follows that

$$m_1 = x^2 - x \text{ and } m_2 = \frac{x^2 - 1}{2x}.$$

The initial equation becomes

$$[m - (x^2 - x)]\left[m - \frac{x^2-1}{2x}\right] = 0.$$

Hence

$$x^2 - x - m = 0, \text{ with solutions } x_{1,2} = \frac{1 \pm \sqrt{1+4m}}{2}$$

and

$$x^2 - 2mx - 1 = 0, \text{ with solutions } x_{3,4} = m \pm \sqrt{1+m^2}.$$

Example 1.24. *Factorize*

$$E(a,b,c) = a^2(b+c) + b^2(c+a) + c^2(a+b) + 2abc.$$

Solution 1. Let us look at $E(a,b,c)$ as at a quadratic polynomial in a and get

$$E(a,b,c) = (b+c)a^2 + (b^2+c^2+2bc)a + b^2c + c^2b.$$

The discriminant of $E(a,b,c) = 0$ is

$$\Delta = (b+c)^4 - 4bc(b+c)^2 = (b+c)^2(b-c)^2 = [(b+c)(b-c)]^2,$$

and the roots are $a_1 = -c$ and $a_2 = -b$. It follows

$$E(a,b,c) = (b+c)(a+b)(a+c).$$

Solution 2. As in previous solution, we have

$$E(a,b,c) = (b+c)a^2 + (b+c)^2a + bc(b+c),$$

hence

$$\begin{aligned} E(a,b,c) &= (b+c)[a^2 + (b+c)a + bc] \\ &= (b+c)[a(a+b) + c(a+b)] = (b+c)(a+b)(a+c). \end{aligned}$$

Example 1.25. *Factorize* $x^2(y-z) + y^2(z-x) + z^2(x-y)$.

Solution. Let $E(x,y,z) = x^2(y-z) + y^2(z-x) + z^2(x-y)$ and write

$$E(x,y,z) = (y-z)x^2 + (z^2-y^2)x + y^2z - z^2y.$$

The discriminant of $E(x,y,z) = 0$ is

$$\begin{aligned} \Delta &= (z^2-y^2)^2 - 4(y-z)(y^2z - z^2y) = (z^2-y^2)^2 - 4yz(y-z)^2 \\ &= (y-z)^2(y-z)^2 = (y-z)^4. \end{aligned}$$

It follows $x_1 = y$, $x_2 = z$ and we get

$$E(x,y,z) = (y-z)(x-y)(x-z).$$

Solution 2. We have

$$\begin{aligned} E(x,y,z) &= (y-z)x^2 + (z^2-y^2)x + y^2z - z^2y \\ &= (y-z)[x^2 - (y+z)x + yz] \\ &= (y-z)(x^2 - yx - zx + yz) \\ &= (y-z)[x(x-y) - z(x-y)] \\ &= (y-z)(x-y)(x-z). \end{aligned}$$

Example 1.26. *Factorize*

$$E(a,b) = 2a^2 - b^2 + ab - 5a + b + 2.$$

Solution. Looking at $E(a,b)$ as a quadratic polynomial in a, we have

$$E(a,b) = 2a^2 + (b-5)a - b^2 + b + 2.$$

The discriminant of equation $E(a,b) = 0$ is

$$\Delta = (b-5)^2 + 8(b^2 - b - 2) = 9b^2 - 18b + 9 = 9(b-1)^2.$$

Applying the formulas (1.7) we get the roots $a_1 = \dfrac{b+1}{2}$ and $a_2 = -b + 2$. From the factorization (1.8) it follows

$$E(a,b) = 2\left(a - \frac{b+1}{2}\right)(a + b - 2) = (2a - b - 1)(a + b - 2).$$

Example 1.27. *Factorize*

$$E(a,b,c) = 2a^2 + 4b^2 - c^2 - 6ab + ac.$$

Solution. We proceed in a similar way as in previous example. Let us look at $E(a,b,c)$ as at a quadratic polynomial in a and get

$$E(a,b,c) = 2a^2 - (6b - c)a + 4b^2 - c^2.$$

The discriminant of equation $E(a,b,c) = 0$ is

$$\Delta = (6b - c)^2 - 8(4b^2 - c^2) = 4b^2 - 12bc + 9c^2 = (2b - 3c)^2.$$

From formulas (1.7) we get the roots $a_1 = 2b - c$ and $a_2 = \dfrac{2b + c}{2}$, hence we obtain the factorization

$$E(a,b,c) = 2(a - 2b + c)\left(a - \frac{2b + c}{2}\right) = (a - 2b + c)(2a - 2b - c).$$

Example 1.28. *Factorize the polynomial*

$$P = 2x^4 + x^3 + 3x^2 + x + 2.$$

Solution. We can write

$$P = x^2\left[2\left(x^2 + \frac{1}{x^2}\right) + \left(x + \frac{1}{x}\right) + 3\right].$$

If we denote $x+\dfrac{1}{x}=y$, then $x^2+\dfrac{1}{x^2}=y^2-2$ and we get

$$\begin{aligned}P&=x^2(2y^2+y-1)=x^2(y^2-1+y^2+y)\\&=x^2[(y-1)(y+1)+y(y+1)]=x^2(y+1)(2y-1)\\&=x^2\left(x+\frac{1}{x}+1\right)\left(2x+\frac{2}{x}-1\right)=(x^2+x+1)(2x^2-x+2).\end{aligned}$$

To factorize P into linear factors we solve the quadratic equations

$$x^2+x+1=0 \quad \text{and} \quad 2x^2-x+2=0,$$

and use (1.8). It follows

$$P=\left(x-\frac{-1+i\sqrt{3}}{2}\right)\left(x-\frac{-1-i\sqrt{3}}{2}\right)\left(x-\frac{1+i\sqrt{15}}{4}\right)\left(x-\frac{1-i\sqrt{15}}{4}\right).$$

Example 1.29. *Factorize*

$$E(a,b,c)=2(a^2b^2+b^2c^2+c^2a^2)-(a^4+b^4+c^4).$$

Solution. Consider $E(a,b,c)$ a as polynomial in a, and get

$$E(a,b,c)=-a^4+2(b^2+c^2)a^2-(b^2-c^2)^2.$$

In order to solve the equation $E(a,b,c)=0$, we denote $a^2=x$, and get the discriminant

$$\Delta=4(b^2+c^2)^2-4(b^2-c^2)^2=16b^2c^2.$$

It follows the roots

$$\begin{aligned}x_1&=b^2+c^2+2bc=(b+c)^2\\x_2&=b^2+c^2-2bc=(b-c)^2.\end{aligned}$$

Hence, we obtain the factorization

$$\begin{aligned}E(a,b,c)&=-(x-x_1)(x-x_2)=-[a^2-(b+c)^2][a^2-(b-c)^2]\\&=-(a+b+c)(a-b-c)(a+b-c)(a+c-b)\\&=(a+b+c)(-a+b+c)(a-b+c)(a+b-c).\end{aligned}$$

Remark. If a,b,c are the side lengths of a triangle, then $s=\dfrac{1}{2}(a+b+c)$ is the semiperimeter and the above formula becomes

$$E(a,b,c) = 16K^2,$$

where K is the area of the triangle.

Alternative solution. We can write

$$\begin{aligned} E(a,b,c) &= 4b^2c^2 - (-a^2+b^2+c^2)^2 = [(b+c)^2 - a^2][a^2 - (b-c)^2] \\ &= (a+b+c)(-a+b+c)(a-b+c)(a+c-b). \end{aligned}$$

Example 1.30. *Factorize*

$$E(a,b,c) = a^2(b+c) + b^2(c+a) + c^2(a+b) + 3abc.$$

Solution. Looking to $E(a,b,c)$ as to a quadratic polynomial in a, we have

$$E(a,b,c) = (b+c)a^2 + (b^2+c^2+3bc)a + bc(b+c).$$

The discriminant to the equation $E(a,b,c) = 0$ is

$$\begin{aligned} \Delta &= (b^2+c^2+3bc)^2 - 4bc(b+c)^2 = [(b+c)^2+bc]^2 - 4bc(b+c)^2 \\ &= \Big[(b+c)^2 - bc\Big]^2 = (b^2+bc+c^2)^2, \end{aligned}$$

hence the roots to $E(a,b,c) = 0$ are

$$\begin{aligned} a_1 &= \frac{-(b^2+c^2+3bc) + (b^2+bc+c^2)}{2(b+c)} = -\frac{bc}{b+c}, \\ a_2 &= \frac{-(b^2+c^2+3bc) - (b^2+bc+c^2)}{2(b+c)} = -(b+c). \end{aligned}$$

It follows

$$\begin{aligned} E(a,b,c) &= (b+c)(a-a_1)(a-a_2) = [(b+c)a+bc](a+b+c) \\ &= (a+b+c)(ab+bc+ca). \end{aligned}$$

Alternative solution. We can write

$$\begin{aligned} E(a,b,c) &= a^2(b+c) + abc + b^2(c+a) + abc + c^2(a+b) + abc \\ &= a(ab+bc+ca) + b(ab+bc+ca) + c(ab+bc+ca) \\ &= (ab+bc+ca)(a+b+c). \end{aligned}$$

1.4 Polynomials in one variable

Let $f = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$, $a_n \neq 0$ be a polynomial of degree n. We shall solve problems involving polynomials with integer, rational, real, or complex coefficients $a_0, a_1, \ldots, a_n$. Denoting these sets of polynomials by $\mathbb{Z}[X]$, $\mathbb{Q}[X]$, $\mathbb{R}[X]$, $\mathbb{C}[X]$, respectively, we have the inclusions:

$$\mathbb{Z}[X] \subset \mathbb{Q}[X] \subset \mathbb{R}[X] \subset \mathbb{C}[X].$$

Every set of polynomials has specific properties. When not mentioned otherwise, the polynomial f is assumed to belong to the largest set, that is $\mathbb{C}[X]$. The number x_0 is a **root** of f if $f(x_0) = 0$.

Theorem 1.1. *(Bézout) The number x_0 is a root of polynomial f if and only if $X - x_0 \mid f(X)$.*

Proof. By the Euclidean division for polynomials one can write the identity $f(X) = (X - x_0)g(X) + r$, where r is a polynomial of degree zero, i.e., a number. Passing to polynomial functions we obtain $f(x_0) = r$. It follows that we have $f(x_0) = 0$ if and only if $r = 0$. □

A corollary of this simple result is the so-called remainder theorem: The remainder of the division of the polynomial f by $X - x_0$ is the evaluation of the polynomial function in x_0, namely $f(x_0)$.

Theorem 1.2. *Let f be a polynomial and $x_1, x_2, \ldots, x_m$ distinct numbers such that $f(x_1) = f(x_2) = \ldots = f(x_m) = 0$. Then $(X - x_1)(X - x_2)\cdots(X - x_m) \mid f(X)$. Particulary, the number of roots of f is not greater than $deg(f)$.*

Proof. From $f(X) = (X - x_1)g_1(X)$ one obtains $(x_2 - x_1)g_1(x_2) = 0$. Since $x_2 \neq x_1$, one has $g_1(x_2) = 0$, which gives $g_1(X) = (X - x_2)g_2(X)$. In this way we get $f(X) = (X - x_1)(X - x_2)g_2(X)$. We conclude by induction. □

Theorem 1.3. *(Fundamental Theorem of Algebra) Every polynomial with complex coefficients has a root in $\mathbb{C}$.*

The proof of this deep result is not elementary and will be skipped. As a consequence of this theorem it follows, by induction, that every polynomial with complex coefficients f can be decomposed in linear factors in $\mathbb{C}[X]$ as

$$f(X) = a_n(X - x_1)(X - x_2)\cdots(X - x_n),$$

where $x_1, x_2, \ldots, x_n$ are the roots of f. Hence, only linear polynomials are irreducible in $\mathbb{C}[X]$.

Recall that the following polynomials in n variables are called the **fundamental symmetric polynomials** of $x_1, x_2, \ldots, x_n$:

$$\begin{aligned}
s_1(x_1,\ldots,x_n) &= x_1 + x_2 + \cdots + x_n \\
s_2(x_1,\ldots,x_n) &= \sum_{1\le i<j\le n} x_i x_j \\
&\cdots \\
s_k(x_1,\ldots,x_n) &= \sum_{1\le i_1<i_2<\ldots<i_k\le n} x_{i_1}x_{i_2}\cdots x_{i_k} \\
&\cdots \\
s_n(x_1,\ldots,x_n) &= x_1x_2\cdots x_n.
\end{aligned}$$

The following relations connecting the fundamental symmetric polynomials of the roots $x_1, x_2, \ldots, x_n$ of polynomial f to the coefficients of f are known as *Vieta's* relations:

$$\begin{aligned}
s_1(x_1,\ldots,x_n) &= x_1 + x_2 + \cdots + x_n = -\frac{a_{n-1}}{a_n} \\
s_2(x_1,\ldots,x_n) &= \sum_{1\le i<j\le n} x_i x_j = \frac{a_{n-2}}{a_n} \\
s_k(x_1,\ldots,x_n) &= \sum_{1\le i_1<i_2<\ldots<i_k\le n} x_{i_1}x_{i_2}\cdots x_{i_k} = (-1)^k\frac{a_{n-k}}{a_n} \\
s_n(x_1,\ldots,x_n) &= x_1x_2\cdots x_n = (-1)^n\frac{a_0}{a_n}.
\end{aligned}$$

Let us now present a few example problems.

Example 1.31. *Determine the polynomials P for which $16P(x^2) = P(2x)^2$.*

Solution 1. Setting $x = 0$ yields $16P(0) = P(0)^2$, i.e. $P(0) = 0$ or 16.

Case 1. Suppose that $P(0) = 0$. Then $P(x) = xQ(x)$ for some polynomial Q and $16x^2Q(x^2) = 4x^2Q(2x)^2$, which reduces to $4Q(x^2) = Q(2x)^2$. Now setting $4Q(x) = R(x)$ gives us $16R(x^2) = R(2x)^2$. Hence, $P(x) = \frac{1}{4}xR(x)$, with R satisfying the same relation as P.

Case 2. Suppose that $P(0) = 16$. Putting $P(x) = xQ(x) + 16$ in the relation we obtain $4xQ(x^2) = xQ(2x)^2 + 16Q(2x)$; hence $Q(0) = 0$, *i.e.* $Q(x) = xQ_1(x)$ for some polynomial Q_1. Furthermore, $x^2Q_1(x^2) = x^2Q_1(2x)^2 + 8Q_1(2x)$, implying that $Q_1(0) = 0$, so Q_1 too is divisible by x. Thus $Q(x) = x^2Q_1(x)$.

Now assume that x^n is the highest degree of x dividing Q, and $Q(x) = x^nR(x)$, where $R(0) \neq 0$. Then R satisfies $4x^{n+1}R(x^2) = 2^{2n}x^{n+1}R(2x)^2 + 2^{n+4}R(2x)$, hence $R(0) = 0$, a contradiction. It follows that $Q = 0$ and $P(x) = 16$. We conclude that $P(x) = 16\left(\frac{1}{4}x\right)^n$ for some positive integer n.

Solution 2. We use the following simple result.

Lemma 1.1. *If $P(x)^2$ is a polynomial in x^2, then so is either $P(x)$ or $P(x)/x$.*

Proof. Let $P(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0, a_n \neq 0$. The coefficient of x^{2n-1} is $2a_n a_{n-1}$, from which we get $a_{n-1} = 0$. The coefficient of x^{2n-3} is $2a_n a_{n-3}$, hence $a_{n-3} = 0$, and so on. After more steps, one obtains $a_{n-2k-1} = 0$ for $k = 0,1,2,\ldots$, that is $P(x) = a_n x^n + a_{n-2}x^{n-2} + a_{n-4}x^{n-4} + \cdots$. □

Since $P(x)^2 = 16P(\frac{x^2}{4})$ is a polynomial in x^2, we have $P(x) = Q(x^2)$ or $P(x) = xQ(x^2)$. In the former case we get $16Q(x^4) = Q(4x^2)^2$ and therefore $16Q(x^2) = Q(4x)^2$; in the latter case we similarly get $4Q(x^2) = Q(4x)^2$. In either case, $Q(x) = R(x^2)$ or $Q(x) = xR(x^2)$ for some polynomial R, so $P(x) = x^i R(x^4)$ for some $i \in \{0,1,2,3\}$. Proceeding in this way we find that $P(x) = x^i S(x^{2^k})$ for each positive integer k and some $i \in \{0,1,\ldots,2^k\}$.

Now it suffices to take k with $2^k > \deg P$ and to conclude that S must be constant. Thus $P(x) = cx^i$ for some constant c. A simple verification gives us the general solution $P(x) = 16\left(\frac{1}{4}x\right)^n$ for some positive integer n.

Example 1.32. *Find all polynomials P with $P(x)^2 + P\left(\frac{1}{x}\right)^2 = P(x^2)P\left(\frac{1}{x^2}\right)$.*

Solution. By Lemma 1.1, there is a polynomial Q with $P(x) = Q(x^2)$ or $P(x) = xQ(x^2)$. In the former case $Q(x^2)^2 + Q\left(\frac{1}{x^2}\right) = Q(x^4)Q\left(\frac{1}{x^4}\right)$, hence $Q(x)^2 + Q\left(\frac{1}{x}\right) = Q(x^2)Q\left(\frac{1}{x^2}\right)$ (which is precisely the relation fulfilled by P), whereas in the latter case (similarly)

$$xQ(x)^2 + \frac{1}{x}Q\left(\frac{1}{x}\right)^2 = Q(x^2)Q\left(\frac{1}{x}\right)$$

which is impossible for the left and right hand side have odd and even degrees, respectively. We conclude that $P(x) = Q(x^2)$, where Q is also a solution of the considered polynomial equation. Considering the solution of the least degree we find that P.

Example 1.33. *Find the non-linear polynomials P and Q with the property*

$$P(Q(x)) = (x-1)(x-2)\cdots(x-15).$$

Solution. Suppose there exist such polynomials. Then $\deg P \cdot \deg Q = 15$, so $\deg P = k \in \{3,5\}$. Putting $P(x) = c(x-a_1)\cdots(x-a_k)$ we deduce that $c(Q(x)-a_1)\cdots(Q(x)-a_k) = (x-1)(x-2)\cdots(x-15)$. Thus the roots of polynomial $Q(x) - a_i$ are distinct and contained the set $\{1,2,\ldots,15\}$. All these polynomials mutually differ at the last coefficient only. Now, investigating parity of the remaining (three or five) coefficients we conclude that each of them has the equally many odd roots. This is impossible, since the total number of odd roots is 8, not divisible by 3 or 5.

Example 1.34. *Determine all the polynomials P with $P(x)^2 - 2 = 2P(2x^2 - 1)$.*

Solution. Denoting $P(1) = a$, we have $a^2 - 2a - 2 = 0$. By substituting $P(x) = (x-1)P_1(x) + a$ in the initial relation and simplifying yields the relation $(x-1)P_1(x)^2 + 2aP_1(x) = 4(x+1)P_1(2x^2-1)$. For $x = 1$ we have $2aP_1(1) = 8P_1(1)$, which (as $a \neq 4$) gives $P_1(1) = 0$, i.e., $P_1(x) = (x-1)P_2(x)$, hence $P(x) = (x-1)^2P_2(x) + a$. Suppose that $P(x) = (x-1)^nQ(x) + a$, where $Q(1) \neq 0$. Substituting in the initial relation and simplifying yields $(x-1)^{2n}Q(x)^2 + 2aQ(x) = 2(2x+2)^nQ(2x^2-1)$, giving us $Q(1) = 0$, a contradiction. It follows that $P(x) = a$.

Example 1.35. *Determine all polynomials P with $P(x)^2 - 1 = 4P(x^2 - 4x + 1)$.*

Solution. Suppose that P is not constant. Fixing $\deg P = n$ and comparing coefficients of both sides we deduce that the coefficients of polynomial P must be rational. On the other hand, setting $x = a$ with $a = a^2 - 4a + 1$, that is, $a = \frac{5\pm\sqrt{21}}{2}$, we obtain $P(a) = b$, where $b^2 - 4b - 1 = 0$, i.e. $b = 2 \pm \sqrt{5}$. However, this is impossible because $P(a)$ must have the form $p + q\sqrt{21}$ for some $p, q \in \mathbb{Q}$, as the coefficients of P are rational. Hence, $P(x)$ is constant.

Example 1.36. *Identify all the polynomials P which satisfy the property $P(x^2 + 1) = P(x)^2 + 1$ for all x.*

Solution. By Lemma 1.1, there is a polynomial Q such that $P(x) = Q(x^2+1)$ or $P(x) = xQ(x^2+1)$. Then $Q((x^2+1)^2+1) = Q(x^2+1)^2 - 1$, from where $(x^2+1)Q((x^2+1)^2+1) = x^2Q(x^2+1)^2 + 1$, respectively. Taking $x^2 + 1 = y$ yields $Q(y^2+1) = Q(y)^2 + 1$ and $yQ(y^2+1) = (y-1)Q(y)^2 + 1$, respectively. Assume that $yQ(y^2+1) = (y-1)Q(y)^2 + 1$ and set $y = 1$ we to obtain $Q(2) = 1$. Note that, if $a \neq 0$ and $Q(a) = 1$, then also $aQ(a^2+1) = (a-1) + 1$ and hence $Q(a^2+1) = 1$. We thus obtain an infinite sequence of points where Q is 1, namely the sequence given by $a_0 = 2$ and $a_{n+1} = a_n^2 + 1$. Therefore $Q = 1$. It follows that if $Q \neq 1$, then $P(x) = Q(x^2+1)$. Now we can easily list all solutions: these are the polynomials of the form $T(T(\cdots(T(x))\cdots))$, where $T(x) = x^2 + 1$.

Example 1.37. *If a polynomial P with real coefficients satisfies for all x*

$$P(\cos x) = P(\sin x),$$

prove that there exists a polynomial Q such that for all x, $P(x) = Q(x^4 - x^2)$.

Solution. By the hypothesis we have $P(-\sin x) = P(\sin x)$, so $P(-t) = P(t)$ for infinitely many t; hence the polynomials $P(x)$ and $P(-x)$ coincide. Therefore $P(x) = S(x^2)$ for some polynomial S. Now $S(\cos^2 x) = S(\sin^2 x)$ for all x, so $S(1-t) = S(t)$ for infinitely many t, hence $S(x) = S(1-x)$.

From here we get $R(x-\frac{1}{2}) = R(\frac{1}{2}-x)$, i.e. $R(y) = R(-y)$, where R is defined by $S(x) = R(x-\frac{1}{2})$. Now $R(x) = T(x^2)$ for some polynomial T, and finally, $P(x) = S(x^2) = R(x^2-\frac{1}{2}) = T(x^4 - x2 + \frac{1}{4}) = Q(x^4-x^2)$ for some polynomial Q.

Example 1.38. *Let f be a quadratic polynomial. Prove that there exist quadratic polynomials g and h such that $f(x)f(x+1) = g(h(x))$.*

Solution. Let $f(x) = a(x-r)(x-s)$. Since

$$f(x)f(x+1) = a^2\{[x^2-(r+s-1)x+rs]-r\}\{[x^2-(r+s-1)x+rs]-s\},$$

we are done by setting $g(x) = a^2(x-r)(x-s), h(x) = x^2-(r+s-1)x+rs$.

Example 1.39. *Prove that any polynomial with real coefficients is the difference of some two increasing polynomial functions (over the reals).*

Solution. Let $P(x) = a_0 + a_1X + \cdots + a_nx^n$. Then

$$\begin{aligned}|P'(x)| &= |a_1 + 2a_2x + \cdots + na_nx^{n-1}| \le |a_1| + 2|a_2||x| + \cdots + n|a_n||x^{n-1}| \\ &< M(1+|x|+\cdots+|x|^{n-1}),\end{aligned}$$

where $M > \max(|a_1|, 2|a_2|, n|a_n|)$. If $|x| \le 1$ then $1+|x|+\cdots+|x|^{n-1} \le n$, and if $|x| > 1$ then $1+|x|+\cdots+|x|^{n-1} < nx^{2n}$. Hence, for any real number x, we have $|P'(x)| < Mn(1+x^{2n})$. Consider the polynomials

$$P_1(x) = P(x) + Mn(x+x^{2n+1}), P_2(x) = Mn(x+x^{2n+1}).$$

We have $P(x) = P_1(x) - P_2(x)$. Also, P_1 and P_2 are increasing functions, as

$$P_1'(x) = P'(x) + Mn(1+(2n+1)x^{2n}) > P'(x) + Mn(1+x^{2n}) > 0$$

and $P_2(x) = Mn((1+(2n+1)x^{2n}) > 0$ for any $x \in \mathbb{R}$.

Example 1.40. *Prove that if the polynomials $P, Q \in \mathbb{R}[X]$ have a real root each and for every $x \in \mathbb{R}$*

$$P(1+x+Q(x)^2) = Q(1+x+P(x)^2),$$

then $P = Q$.

Solution. Note that there exists $x = a$ for which $P(a)^2 = Q(a)^2$. This follows from the fact that, if p and q are the respective real roots of P and Q, then $P(p)^2 - Q(p)^2 \le 0 \le P(q)^2 - Q(q)^2$, and moreover the function $P^2 - Q^2$ is continuous. Now $P(b) = Q(b)$ for $b = 1+a+P(a)^2$. Taking a to be the largest real number for which $P(a) = Q(a)$ leads to an immediate contradiction.

Example 1.41. *Prove that not all zeros of $x^n + 2nx^{n-1} + 2n^2x^{n-2} + \cdots$, are real.*

Solution. Suppose that all its zeros $x_1, x_2, \ldots, x_n$ are real. They satisfy

$$\sum_{i=1}^{n} x_i = -2n, \quad \sum_{i<j} x_i x_j = 2n^2.$$

However, by the mean inequality we have

$$2n^2 = \sum_{i<j} x_i x_j = \frac{1}{2}\left(\sum_{i=1}^{n} x_i\right)^2 - \frac{1}{2}\sum_{i=1}^{n} x_i^2 \leq \frac{n-1}{2n}\left(\sum_{i=1}^{n} x_i\right)^2 = 2n(n-1),$$

a contradiction.

Example 1.42. *Find all the polynomials $a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ such that $a_j \in \{-1, 1\}$, $j = 0, 1, \ldots, n$, whose all roots are real.*

Solution. Let $x_1, \ldots, x_n$ be the roots of the given polynomial. Then

$$x_1^2 + x_2^2 + \cdots + x_n^2 = \left(\sum_{i=1}^{n} x_i\right)^2 - 2\left(\sum_{i<j} x_i x_j\right) = a_{n-1}^2 - 2a_{n-2} \leq 3.$$

By the mean inequality, the second equality implies $x_1^2 + \cdots + x_n^2 \geq n$, hence $n \leq 3$. The case $n = 3$ is only possible if $x_1, x_2, x_3 = \pm 1$. Now we can easily find all solutions: $x \pm 1, x^2 \pm x - 1, x^3 - x \pm (x^2 - 1)$.

Example 1.43. *Solve in the real numbers the system of equations*

$$\begin{cases} x + y + z = 4 \\ x^2 + y^2 + z^2 = 14 \\ x^3 + y^3 + z^3 = 34 \end{cases}.$$

Solution. Consider the monic polynomial

$$P(t) = t^3 + at^2 + bt + c,$$

with roots x, y, z. Because $x + y + z = 4$, it follows that $a = -4$, hence

$$P(t) = t^3 - 4t^2 + bt + c.$$

We have

$$x^2 + y^2 + z^2 = (x + y + z)^2 - 2(xy + xz + yz),$$

from where it follows that $b = xy + xz + yz = 1$. The numbers x, y, z are the roots of P, thus

$$x^3 - 4x^2 + x + c = 0,$$
$$y^3 - 4y^2 + y + c = 0,$$
$$z^3 - 4z^2 + z + c = 0.$$

Adding these equalities and using the system, we obtain $c = 6$, hence

$$P(t) = t^3 - 4t^2 + t + 6.$$

We observe that $t_1 = -1$ is a root, so P factors as

$$P(t) = (t+1)(t^2 - 5t + 6),$$

the other two roots being $t_2 = 2$ and $t_3 = 3$. It follows that the solutions of the system are the triple $(-1,2,3)$ and all of its permutations.

Example 1.44. *Let $x_1, x_2, \ldots, x_n$ be the roots of equation*

$$x^n + 2x^{n-1} + 3x^{n-2} + \cdots + nx + n + 1 = 0.$$

Compute

$$\sum_{k=1}^{n} \frac{x_k^{n+1} - 1}{x_k - 1}.$$

Solution. We can write the equation in the following equivalent form

$$\frac{x^{n+1} - 1}{x - 1} + \frac{x^n - 1}{x - 1} + \cdots + \frac{x^2 - 1}{x - 1} = \frac{x - 1}{x - 1} = 0, \quad x \neq 1,$$

that is

$$\frac{1}{x - 1}[x^{n+1} + x^n + \cdots + x^2 + x - (n+1)] = 0, \quad x \neq 1.$$

We get

$$\frac{1}{x - 1}\left[x \cdot \frac{x^{n+1} - 1}{x - 1} - (n+1)\right] = 0, \quad x \neq 1.$$

It follows that x_k satisfies the relation

$$x_k \cdot \frac{x_k^{n+1} - 1}{x_k - 1} - (n+1) = 0, \quad k = 1,2,\ldots,n$$

hence

$$\frac{x_k^{n+1} - 1}{x_k - 1} = \frac{n+1}{x_k}, \quad k = 1,2,\ldots,n.$$

Then, we have

$$\sum_{k=1}^{n} \frac{x_k^{n+1}-1}{x_k-1} = (n+1)\sum_{k=1}^{n} \frac{1}{x_k}.$$

Note that $\frac{1}{x_1}, \frac{1}{x_2}, \ldots, \frac{1}{x_n}$ are the roots of the equation

$$(n+1)y^n + ny^{n-1} + \cdots + 2y + 1 = 0,$$

hence we have

$$\frac{1}{x_1} + \frac{1}{x_2} + \cdots + \frac{1}{x_n} = -\frac{n}{n+1},$$

and we get

$$\sum_{k=1}^{n} \frac{x_k^{n+1}-1}{x_k-1} = (n+1)\left(-\frac{n}{n+1}\right) = -n.$$

Example 1.45. *Find the roots of the polynomial*

$$f(X) = X^{10} - 10X^9 + 45X^8 + a_7X^7 + \cdots + a_1X + a_0,$$

assuming that they are all real numbers.

Solution. We have $\sum_{i=1}^{10} x_i = 10$ and $\sum x_i x_j = 45$. Compute

$$\sum_{i=1}^{10}(x_i-1)^2 = \sum_{i=1}^{10} x_i^2 - 2\sum_{i=1}^{10} x_i + 10 = 0.$$

Since all roots are real, it follows that $x_1 = \cdots = x_{10} = 1$.

Example 1.46. *Solve the system*

$$\begin{cases} x+y+z=1 \\ xyz=1 \end{cases}$$

for x, y and z complex numbers of modulus 1.

Solution. Since $\overline{x} = \frac{1}{x}$, from the first equation we have that

$$\frac{1}{x} + \frac{1}{y} + \frac{1}{z} = 1,$$

which gives $xy + yz + zx = 1$. Hence, x, y, z are the roots of the polynomial

$$T^3 - T^2 + T - 1 = 0.$$

It is easy to see that the latter has the roots $1, i, -i$.

Example 1.47. *Solve the systems of equations:*

$$(a)\quad \begin{cases} x+y+z=4 \\ x^2+y^2+z^2=14 \\ x^3+y^3+z^3=34. \end{cases}$$

$$(b)\quad \begin{cases} x^3-9y^2+27y-27=0 \\ y^3-9z^2+27z-27=0 \\ z^3-9x^2+27x-27=0. \end{cases}$$

Solution. (a) Consider the cubic equation with roots x,y,z. This is

$$(T-x)(T-y)(T-z)=T^3+aT^2+bT+c=0,$$

where the coefficients a,b,c are given by Viète formulas:

$$\begin{aligned} a &= -(x+y+z)=-4 \\ b &= xy+yz+zx=(1/2)[(x+y+z)^2-(x^2+y^2+z^2)=1 \\ c &= -xyz \\ &= \frac{1}{3}\left[(x^3+y^3+z^3)-(x+y+z)^3+3(x+y+z)(xy+yz+zx)\right]=6. \end{aligned}$$

One obtains the equation $T^3-4T^2+T+6=0$, which has the roots -1, 2, and 3. Any permutation of this set is a solution of the system.

(b) Sum the equations to obtain

$$(x-3)^3+(y-3)^3+(z-3)^3=0.$$

From the first equation we have

$$x^3=9(y^2-3y+3)$$

giving that $x\geq 0$. Similarly, $y\geq 0$ and $z\geq 0$. Assume that $x>3$. From the first equation we get $x^3-27=9y(y-3)$, yielding that $y>3$. Similarly one obtains $z>3$. This gives a contradiction with the sum of cubes which is zero. Analogously, $x<3$ gives a contradiction. So, the solution is $x=y=z=3$.

Example 1.48. *Prove that the set of real numbers x for which $\sum_{k=1}^{70}\frac{k}{x-k}\geq\frac{5}{4}$ is a disjoint union of intervals. Compute the sum of the lengths of all these intervals.*

Solution. Consider the function $f:\mathbb{R}\setminus\{1,2,\ldots,70\}\longrightarrow\mathbb{R}$ given by

$$f(x)=\sum_{k=1}^{70}\frac{k}{x-k}.$$

This function is decreasing on all intervals in its domain. The limit towards the points $x = 1,2,\ldots,70$ is $-\infty$ from the left and $+\infty$ from the right. The inequality therefore holds on the union of intervals $\bigcup_{k=1}^{70}(k, x_k]$, where x_k are the points in which $f(x_k) = \frac{5}{4}$. The equation $f(x) = \frac{5}{4}$ is equivalent to

$$5\prod_{k=1}^{70}(x-k) - 4\sum_{k=1}^{70} k(x-1)\cdots(x-k+1)(x-k-1)\cdots(x-70) = 0.$$

We are asked to find the sum of length of intervals which is

$$l = \sum_{k=1}^{70}(x_k - k) = \sum_{k=1}^{70} x_k - \sum_{k=1}^{70} k.$$

So we have to compute only the sum of roots. The equation has degree 70. Using Viète formulas we obtain:

$$l = \frac{1}{5}\left(5\sum k + 4\sum k\right) - \sum k = \frac{4}{5}\sum k = 1988.$$

Example 1.49. *Let a, b, c, d, e and f be positive integers. Suppose that the sum $S = a+b+c+d+e+f$ divides both $ab+bc+ca-de-ef-fd$ and $abc+def$. Show that S is a composite number.*

Solution. Consider the quadratic polynomial

$$P(X) = (X+a)(X+b)(X+c) - (X-d)(X-e)(X-f) =$$

$$(a+b+c+d+e+f)X^2 + (ab+bc+ca-de-ef-fd)X + abc+def.$$

Its coefficients are all integers divisible by S. It follows that $S|P(d) = (d+a)(d+b)(d+c)$. If S is prime number, then S divides one of the factors of $P(d)$, which is a contradiction.

Example 1.50. *Let a,b,c,d be positive real numbers. Show that the following inequalities cannot hold simultaneously:*

$$\begin{aligned} a+b &< c+d, \\ (a+b)(c+d) &< ab+cd, \\ (a+b)cd &< (c+d)ab. \end{aligned}$$

Solution. Consider the real polynomial

$$P(X) = (X-a)(X-b)(X+c)(X+d) = X^4 + (-a-b+c+d)X^3 +$$

$$(ab+cd-ac-bc-ad-bd)X^2 + (abc+abd-acd-bcd)X + abcd.$$

Assuming that all coefficients are positive, we get that $P(x) > 0$ for all $x > 0$. This contradicts the fact that P has positive roots a, b, hence the conclusion.

1.4.1 Chebyshev polynomials

Chebyshev polynomials $T_n(x)$ are one of the most remarkable families of polynomials, which appear in various branches of mathematics. In this section we discuss several simple but important properties of the Chebyshev polynomials, starting from the definition based on the fact that $\cos nx$ can be expressed as a polynomial of $\cos x$, i.e., there exists a polynomial $T_n(x)$ such that $T_n(x) = \cos nt$ for $x = \cos t$. Indeed, the formula

$$\cos(n+1)t + \cos(n-1)t = 2\cos t \cos nt$$

shows that the polynomials $T_n(x)$ recursively defined by the relation

$$T_{n+1}(x) = 2xT_n(x) - T_{n-1}(x)$$

with the initial values $T_0(x) = 1$ and $T_1(x) = x$, possess the property required. These polynomials $T_n(x)$ are called the **Chebyshev polynomials**. The fact that $T_n(x) = \cos nt$ for $x = \cos t$ directly implies that $|T_n(x)| \le 1$ for $|x| \le 1$. The above recurrence implies that

$$T_n(x) = 2^{n-1}x^n + a_1x^{n-1} + \cdots + a_n,$$

where $a_1, \ldots, a_n$ are integers.

The most important property of Chebyshev polynomials was discovered by Chebyshev himself. It consists of the following.

Theorem 1.4. *Let $P_n(x) = x^n + \cdots$ be a monic polynomial of degree n such that $|P_n(x)| \le \frac{1}{2^{n-1}}$ for $|x| \le 1$. Then $P_n(x) = \frac{T_n(x)}{2^{n-1}}$, i.e., the polynomial $\frac{T_n(x)}{2^{n-1}}$ is the monic polynomial of degree n with the least deviation from zero on $[-1,1]$.*

Proof. We use only one property of the polynomial, namely, the fact that

$$T_n\left(\cos\frac{k\pi}{n}\right) = \cos k\pi = (-1)^k, k = 0,1,\ldots,n.$$

Consider the polynomial

$$Q(x) = \frac{T_n(x)}{2^{n-1}} - P_n(x).$$

Its degree does not exceed $n-1$ as the leading terms of $\frac{T_n(x)}{2^{n-1}}$ and $P_n(x)$ are equal. Since $|P_n(x)| \le \frac{1}{2^{n-1}}$ for $|x| \le 1$, at the point $x_k = \cos\frac{k\pi}{n}$ the sign of $Q(x_k)$ coincides with the sign of $T_n(x_k)$. Therefore, at the end points of each segment $[x_{k+1}, x_k]$, the polynomial $Q(x)$ takes values of opposite signs, and hence $Q(x)$ has a root on each of these segments.

If $Q(x_k) = 0$ we need a slightly more accurate arguments. In this case either x_k is a double root or within one of the segments $[x_{k+1}, x_k]$ and $[x_k, x_{k-1}]$

there is one more root. This follows from the fact that the values $Q(x_{k+1})$ and $Q(x_{k-1})$ have the same sign. The number of segments $[x_{k+1}, x_k]$ is equal to n, and hence the polynomial $Q(x)$ has at least n roots. A polynomial of degree not greater than $n-1$ must be identically zero, i.e., $P_n(x) = \frac{T_n(x)}{2^{n-1}}$. □

If $z = \cos t + i \sin t$, then $z + z^{-1} = 2\cos t$ and $z^n + z^{-n} = 2\cos nt$. Therefore $T_n\left(\frac{z+z^{-1}}{2}\right) = \frac{z^n+z^{-n}}{2}$. By this property we can prove the following statement.

Theorem 1.5. *Let $m = \left\lfloor \frac{n}{2} \right\rfloor$. Then*

$$T_n(x) = \sum_{j=0}^{m} \binom{n}{2j} x^{n-2j} \left(x^2 - 1\right)^j.$$

Proof. Let $x = \frac{z+z^{-1}}{2}$ and $y = \frac{z-z^{-1}}{2}$. Then $y^2 = x^2 - 1$ and

$$\begin{aligned} z^n + z^{-n} = (x+y)^n + (x-y)^n &= \sum_{i=0}^{n} \binom{n}{i} \left(1 + (-1)^i\right) x^{n-i} y^i \\ &= 2\sum_{j=0}^{m} \binom{n}{2j} x^{n-2j} y^{2j} = 2\sum_{j=0}^{m} \binom{n}{2j} x^{n-2j} \left(x^2 - 1\right)^j. \end{aligned}$$

It remains to observe that $T_n(x) = \frac{z^n+z^{-n}}{2}$. □

Corollary 1.1. *Let p be an odd prime. Then $T_p(x) \equiv T_1(x) \pmod{p}$.*

Proof. We write $p = 2m + 1$. Then $T_p(x) = \sum_{j=0}^{m} \binom{p}{2j} x^{n-2j}(x^2-1)^j$. If $j > 0$, then $\binom{p}{2j}$ is divisible by p. So $T_p(x) \equiv x^p \pmod{p} \equiv x \pmod{p} = T_1(x)$. □

For any pair of polynomials P and Q, define their composition naturally, by setting $(P \circ Q)(x) = P(Q(x))$. The polynomials P and Q are said to commute if $P \circ Q = Q \circ P$, i.e., if $P(Q(x)) = Q(P(x))$.

Theorem 1.6. *The polynomials $T_n(x)$ and $T_m(x)$ commute.*

Proof. Let $x = \cos t$. Then $T_n(x) = \cos(nt) = y$ and $T_m(y) = \cos m(nt)$, and hence $T_m(T_n(x)) = \cos mnt$. Similarly, $T_n(T_m(x)) = \cos mnt$. Hence the identity $T_n(T_m(x)) = T_m(T_n(x))$ holds for $|x| < 1$, hence it holds for all x. □

Sometimes instead of $T_n(x)$ it is convenient to consider the monic polynomial $P_n(x) = 2T_n(\frac{x}{2})$. The polynomials $P_n(x)$ satisfy the recurrence relation

$$P_{n+1}(x) = xP_n(x) - P_{n-1}(x).$$

Hence $P_n(x)$ is a polynomial with integer coefficients. If $z = \cos t + i \sin t$, then $z + z^{-1} = 2\cos t$ and $z^n + z^{-n} = 2\cos nt$. Therefore

$$P_n(z+z^{-1}) = 2T_n(\cos t) = 2\cos nt = z^n + z^{-n},$$

i.e., the polynomial $P_n(x)$ expresses $z^n + z^{-n}$ via $z + z^{-1}$. Using the polynomials P_n we can prove another result.

Theorem 1.7. *If both α and $\cos(\alpha\pi)$ are rational, then $2\cos(\alpha\pi)$ is an integer, i.e., $\cos(\alpha\pi) = 0, \pm\frac{1}{2}$ or ± 1.*

Proof. Let $\alpha = \frac{m}{n}$ be an irreducible fraction. Set $x_0 = 2\cos t$, where $t = \alpha\pi$. Then $P_n(x_0) = 2\cos(nt) = 2\cos(n\alpha\pi) = 2\cos(m\pi) = \pm 2$. Hence x_0 is a root of the integral polynomial $P_n(x) \mp 2 = x^n + b_1 x^{n-1} + \cdots + b_n$.

Let $x_0 = 2\cos(\alpha\pi) = \frac{p}{q}$ be an irreducible fraction. Then it follows that $p^n + b_1 p^{n-1} q + \cdots + b_n q^n = 0$, and hence p^n is divisible by q. But p and q are relatively prime, and so $q = \pm 1$, i.e., $2\cos(\alpha\pi)$ is an integer. □

In problems concerning extremal properties of polynomials, Chebyshev polynomials play a very special role, as seen in the examples below.

Example 1.51. *Find the maximal value of the expression $a^2 + b^2 + c^2$ provided that $|ax^2 + bx + c| \le 1$ for all $x \in [-1,1]$.*

Solution. Define

$$A = f(1), \quad B = f(0), \quad C = f(-1).$$

Then we easily obtain

$$a = \frac{A+C}{2} - B, \quad b = \frac{A-C}{2}, \quad c = B.$$

Therefore, an immediate computation gives

$$a^2 + b^2 + c^2 = \frac{A^2 + C^2}{2} + 2B^2 - B(A+C).$$

Since $|A|, |B|, |C| \le 1$, the last expression is clearly bounded above by 5 (use the obvious estimate for each term of it). Thus, we shall have $a^2 + b^2 + c^2 \le 5$. To see that it is optimal, simply take Chebyshev's polynomial $2X^2 - 1$.

Example 1.52. *Define $F(a,b,c) = \max\limits_{x\in[0,3]} |x^3 - ax^2 - bx - c|$. What is the least possible value of this function over $\mathbb{R}^3$?*

Solution. Let $P_{a,b,c}(X) = X^3 - aX^2 - bX - c$. The idea is to map the interval $[0,3]$ to $[-1,1]$ via an affine map and then to use Chebyshev's least deviation theorem in order to bound from below $\max_{x\in[0,3]} |P_{a,b,c}(x)|$. Note that

$$\max_{x\in[0,3]} |P_{a,b,c}(x)| = \max_{x\in[-1,1]} \left| P_{a,b,c}\left(\frac{3(x+1)}{2}\right)\right|.$$

Since $P_{a,b,c}\left(\frac{3(X+1)}{2}\right)$ is a polynomial of third degree with leading coefficient $27/8$, Chebyshev's theorem gives us the estimate

$$\max_{x\in[-1,1]} |P_{a,b,c}\left(\frac{3(x+1)}{2}\right)| \geq \frac{27}{32},$$

which is optimal. Bring this to $[0,3]$ we get $F(a,b,c) \geq \frac{27}{32}$ which is optimal, since equality holds for $P_{a,b,c} = \frac{27}{32}T_3(2X/3-1)$, where $T_3(X) = 4X^3 - 3X$.

Example 1.53. *Let $a,b,c,d \in \mathbb{R}$ with $|ax^3+bx^2+cx+d| \leq 1$ for all $x \in [-1,1]$. Prove that*

$$|a|+|b|+|c|+|d| \leq 7.$$

Solution 1. Let us look at the values of $P(X) = aX^3+bX^2+cX+d$ at $-1,-1/2,1/2,1$, which are the classical interpolation points in Chebyshev's theorem (for $n=3$). Writing

$$A = f(1), \quad B = f(1/2), \quad C = f(-1/2), \quad D = f(-1),$$

we can express a,b,c,d in terms of A,B,C,D as follows

$$a = \frac{2}{3}(A-D) - \frac{4}{3}(B-C), \quad b = \frac{2}{3}(A-B) - \frac{2}{3}(C-D),$$
$$c = -\frac{1}{6}(A+D) + \frac{4}{3}(B-C), \quad d = -\frac{1}{6}(A+D) + \frac{2}{3}(B+C).$$

This shows that $f(a,b,c,d) = |a|+|b|+|c|+|d|$ is actually a convex function of $A,B,C,D \in [-1,1]$. Thus it attains its maximum when all A,B,C,D are equal to 1 or -1. Now, it is simply a tedious matter to check that in all cases the expression is at most 7. We have equality for the Chebyshev polynomial (or its opposite) of degree 3.

Solution 2. We look again at the points $-1,-1/2,1/2,1$, but in a slightly different way. Let $P(X) = aX^3+bX^2+cX+d$. Since $-P(X)$ and $P(-X)$ also satisfy the same properties as P, we may assume that $a,b \geq 0$. The rest of the proof is a discussion following the signs of c,d. Namely, if $c \geq 0, d \geq 0$, we have

$$|a|+|b|+|c|+|d| = a+b+c+d = P(1) \leq 1.$$

For $c \geq 0, d < 0$ we obtain

$$|a|+|b|+|c|+|d| = a+b+c-d = P(1) - 2P(0) \leq 3,$$

while for $c < 0, d \geq 0$ we can write

$$\begin{aligned} |a|+|b|+|c|+|d| &= a+b-c+d \\ &= \frac{4}{3}P(1) - \frac{1}{3}P(-1) - \frac{8}{3}P\left(\frac{1}{2}\right) + \frac{8}{3}P\left(-\frac{1}{2}\right) \leq 7. \end{aligned}$$

Finally, when $c < 0, d < 0$ we get

$$|a| + |b| + |c| + |d| = a + b - c - d = \frac{5}{3}P(1) - 4P\left(-\frac{1}{2}\right) + \frac{4}{3}P\left(\frac{1}{2}\right) \leq 7.$$

In all cases, the inequality is proved, finishing the solution.

1.4.2 Lagrange interpolating polynomial

A polynomial of degree n is uniquely determined, given its values at $n+1$ points. So, suppose that P is an n-th degree polynomial and that $P(x_i) = y_i$ in different points $x_0, x_1, \ldots, x_n$. There exist unique polynomials $E_0, E_1, \ldots, E_n$ of degree n such that $E_i(x_i) = 1$ and $E_i(x_j) = 0$ for $j \neq i$. Then the polynomial $P(x) = y_0E_0(x) + y_1E_1(x) + \cdots + y_nE_n(x)$ has the desired properties. Indeed, $P(x_i) = \sum_{j=1}^{n} y_jE_j(x_i) = y_iE_i(x_i) = y_i$. It remains to find the polynomials $E_0, \ldots, E_n$. A polynomial that vanishes at the n points $x_j, j \neq i$, is divisible by $\prod_{i \neq j} = (x - x_j)$, from which we easily obtain $E_i(x) = \prod_{i \neq j} \frac{x - x_j}{x_i - x_j}$.

Theorem 1.8. *(Lagrange interpolating polynomial). For given numbers $y_0, \ldots, y_n$ and distinct $x_0, \ldots, x_n$ there is a unique polynomial P of degree n such that $P(x_i) = y_i$ for $i = 0, 1, \ldots, n$. This polynomial is given by the formula*

$$P(x) = \sum_{i=0}^{n} y_i \prod_{i \neq j} \frac{x - x_j}{x_i - x_j}.$$

It is often useful to consider the finite difference of polynomial P defined by $P^{[1]}(x) = P(x+1) - P(x)$, which has the degree smaller by 1 than for P. Further, one can define the k-th finite difference, $P^{[k]} = (P^{[k-1]})^{[1]}$, whose degree is $n - k$, (assuming that $\deg P = n$). Using simple induction one can deduce the general formula

$$P^{[k]} = \sum_{i=0}^{k} (-1)^{k-i} \binom{k}{i} P(x+i).$$

In particular, $P^{[n]}$ is constant and $P^{[n+1]} = 0$, one has the following result.

Theorem 1.9. *The following relation holds*

$$P(x+n+1) = \sum_{i=0}^{n} (-1)^{n-i} \binom{n+1}{i} P(x+i).$$

We now present some illustrative examples.

Example 1.54. *Find the cubic polynomial Q such that $Q(i) = 2i$ for $i = 0,1,2,3$.*

Solution. We have

$$Q(x) = \frac{(x-11)(x-2)(x-3)}{-6} + 2\frac{x(x-2)(x-3)}{2} + 4\frac{x(x-1)(x-3)}{-2} + 8\frac{x(x-1)(x-2)}{6} = \frac{1}{6}(x^3+5x+6).$$

Example 1.55. *Considering the polynomial P of degree n taking the value 1 in points $0,2,4,\ldots,2n$, prove the combinatorial identity:*

$$\sum_{i=1}^{n+1} \frac{(-1)^{n-i}}{(2i+1)i!(n-i)!} = \frac{2^n}{(2n+1)!!}.$$

Solution. $P(x)$ is of course identically equal to 1, so $P(1) = P(-1) = 1$. But if we apply the Lagrange interpolating polynomial, here is what we get:

$$P(1) = \sum_{i=0}^{n}\prod_{j\neq i}\frac{1-2i}{2j-2i} = \sum_{i=0}^{n}\prod_{j\neq i}\frac{-1-2j}{2j-2i} = \frac{(2n+1)!!}{2^n}\sum_{i=1}^{n+1}\frac{(-1)^{n-i}}{(2i+1)i!(n-i)!}.$$

Example 1.56. *A polynomial p of degree n satisfies $p(k) = 2^k$ for all $0 \leq k \leq n$. Find its value at $n+1$.*

Solution. Applying Lagrange's interpolation formula, we obtain

$$p(n+1) = \sum_{k=0}^{n} p(k)\cdot\prod_{j\neq k}\frac{n+1-j}{k-j} = \sum_{k=0}^{n}\binom{n+1}{k}(-1)^{n-k}2^k = 2^{n+1}-1.$$

Remark. There is also a neat solution without the use of interpolation formula: consider the polynomial

$$f(X) = \binom{X}{0} + \binom{X}{1} + \cdots + \binom{X}{n}.$$

It has degree n and satisfies $f(k) = 2^k$ for all $0 \leq k \leq n$, by the binomial formula. Thus, we must have $f = p$ and then clearly $p(n+1) = 2^{n+1}-1$.

Example 1.57. *A polynomial f of degree n satisfies*

$$f(k) = \frac{1}{\binom{n+1}{k}},$$

for all $0 \leq k \leq n$. Find $f(n+1)$.

Solution. This is also immediate using Lagrange's interpolation formula:

$$f(n+1) = \sum_{k=0}^{n} f(k) \prod_{j \neq k} \frac{n+1-j}{k-j} = \sum_{k=0}^{n} \frac{1}{\binom{n+1}{k}} \cdot (-1)^{n-k} \binom{n+1}{k}$$
$$= \sum_{k=0}^{n} (-1)^{n-k} = \frac{1-(-1)^{n+1}}{2}.$$

Example 1.58. *Prove that for any real number a the following identity holds*

$$\sum_{k=0}^{n} (-1)^k \binom{n}{k} (a-k)^n = n!.$$

Solution. Using Lagrange interpolation, we have

$$P(X) = \sum_{k=0}^{n} P(k)(-1)^{n-k} \frac{1}{n!} \binom{n}{k} \prod_{j \neq k} (X-j)$$

for any polynomial P of degree at most n. If we identify the leading coefficients, we obtain that the leading coefficient of $P(X)$ is

$$\frac{1}{n!} \sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} P(k).$$

Applying this to the polynomial $P(X) = (a-X)^n$ yields the desired identity.

Example 1.59. *Prove that*

$$\sum_{k=0}^{n} \frac{x_k^{n+1}}{\prod_{j \neq k} (x_k - x_j)} = \sum_{k=0}^{n} x_k$$

and compute

$$\sum_{k=0}^{n} \frac{x_k^{n+2}}{\prod_{j \neq k} (x_k - x_j)}.$$

Solution. The method below shows how to compute all sums of the form

$$\sum_{k=0}^{n} \frac{x_k^{n+p}}{\prod_{j \neq k} (x_k - x_j)}.$$

The idea is to consider the remainder $f(X)$ of X^{n+p} when divided by $\prod_{j=0}^{n} (X - x_j)$ and to apply Lagrange's interpolation formula to it. Identifying leading coefficients and using that $f(x_j) = x_j^{n+p}$, we deduce that

$$\sum_{k=0}^{n} \frac{x_k^{n+p}}{\prod_{j\neq k}(x_k - x_j)}$$

is precisely the leading coefficient of $f(X)$. For $p = 1$ we clearly have

$$f(X) = X^{n+1} - \prod_{j=0}^{n}(X - x_j),$$

so its leading coefficient is $\sum_{i=0}^{n} x_i$. On the other hand, for $p = 2$ we have

$$X^{n+2} = Q(X)\prod_{j=0}^{n}(X - x_j) + f(X)$$

for some polynomial Q. Comparing degrees and leading coefficients shows that $Q(X) = X + c$ for some constant c. To determine c, we impose the condition that $\deg(f) \leq n$. This implies that $c = \sum_{j=0}^{n} x_j$. Then, it is easy to find the coefficient of X^n in $f(X)$ and the answer is $(\sum_{j=0}^{n} x_j)^2 - \sum_{0\leq i<j\leq n} x_i x_j$. We leave as a nice exercise for the reader to prove that for all p we have

$$\sum_{k=0}^{n} \frac{x_k^{n+p}}{\prod_{j\neq k}(x_k - x_j)} = \sum_{a_1+a_2+\cdots+a_n=p} x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n},$$

where in the sum above the a_i are nonnegative integers.

The next problems involve extremal properties of polynomials. The idea is that imposing conditions on the values of a polynomial at sufficiently many points of an interval automatically imposes conditions at all other values. Lagrange's interpolation formula is a handy tool in such situations.

Example 1.60. *Let a, b, c be real numbers with $\max\{|f(\pm 1)|, |f(0)|\} \leq 1$ where $f(x) = ax^2 + bx + c$. Show that if $|x| \leq 1$ then $|f(x)| \leq \frac{5}{4}$ and $\left|x^2 f\left(\frac{1}{x}\right)\right| \leq 2$.*

Solution. Using Lagrange interpolation, we can write

$$f(X) = f(0)(1 - X^2) + f(1)\frac{X^2 + X}{2} + f(-1)\frac{X^2 - X}{2}.$$

We deduce that for all $|x| \leq 1$ we have

$$|f(x)| \leq 1 - x^2 + \frac{|x^2 + x|}{2} + \frac{|x^2 - x|}{2} = 1 - x^2 + |x| \leq \frac{5}{4},$$

the last inequality being equivalent to $(|x| - \frac{1}{2})^2 \geq 0$. Similarly, we find that

$$|x^2 f(1/x)| \leq 1 - x^2 + \frac{1 + x}{2} + \frac{1 - x}{2} = 2 - x^2 \leq 2.$$

Remark. For third degree polynomials, Chebyshev's theorem can be proved using Lagrange's interpolation formula: if f is a monic polynomial of third degree, identifying leading coefficients in Lagrange's formula yields

$$1 = \frac{2f(-1)}{3} - \frac{4f(1/2)}{3} + \frac{4f(-1/2)}{3} - \frac{2f(-1)}{3}.$$

This equality and the triangle inequality imply that $\max_{x\in[-1,1]} |f(x)| \geq \frac{1}{4}$ for any such f, with equality when $f(X) = X^3 - \frac{3}{4}X$.

Example 1.61. *Let $a,b,c,d \in \mathbb{R}$ satisfying $|ax^3 + bx^2 + cx + d| \leq 1$ for all values $x \in [-1,1]$. What is the maximal value of $|c|$? For which polynomials is the maximum attained?*

Solution. Choose distinct numbers x_0, x_1, x_2, x_3 and identify the coefficients of X in Lagrange's formula

$$aX^3 + bX^2 + cX + d = \sum_{k=0}^{3} f(x_k) \prod_{j\neq k} \frac{X - x_j}{x_k - x_j}.$$

We deduce that

$$c = \sum f(x_0) \frac{x_1x_2 + x_2x_3 + x_3x_1}{(x_0 - x_1)(x_0 - x_2)(x_0 - x_3)},$$

so

$$|c| \leq \sum \left| \frac{x_1x_2 + x_2x_3 + x_3x_1}{(x_0 - x_1)(x_0 - x_2)(x_0 - x_3)} \right|.$$

The problem is to find a 4-tuple (x_0, x_1, x_2, x_3) which minimizes the last expression. One may consider the points where $|T_3(x)|$ takes maximal value, namely 1, on the interval $[-1,1]$. These are the points $x_0 = -1, x_1 = -\frac{1}{2}, x_2 = \frac{1}{2}$ and $x_3 = 1$. It is easy to compute the last sum in this case and we find that $|c| \leq 3$. Since this value is attained for the polynomial $T_3(X) = 4X^3 - 3X$, this is the maximal value. Also, it is not difficult to check that equality appears in the above chain of inequalities only for T_3 and $-T_3$.

Example 1.62. *If a polynomial $f \in \mathbb{R}[X]$ of degree n satisfies $|f(x)| \leq 1$ for all $x \in [0,1]$, then*

$$\left| f\left(-\frac{1}{n}\right) \right| \leq 2^{n+1} - 1.$$

Solution. The idea is to use Lagrange's interpolation formula at the points k/n for $0 \leq k \leq n$, as in this case all expressions have very nice closed forms. Indeed, we have

$$f\left(\frac{-1}{n}\right) = \sum_{k=0}^{n} f\left(\frac{k}{n}\right) \prod_{j\neq k} \frac{-(j+1)}{k-j},$$

which shows that

$$\left|f\left(\frac{-1}{n}\right)\right| \leq \sum_{k=0}^{n}\prod_{j\neq k}\frac{j+1}{|k-j|} = \sum_{k=0}^{n}\binom{n+1}{k+1} = 2^{n+1}-1.$$

Example 1.63. *Let $a \geq 3$ be a real number and p a real polynomial of degree n. Prove that* $\max_{i=0,1,\ldots,n+1}|a^i - p(i)| \geq 1$.

Solution. The crucial observation is that we have

$$\sum_{k=0}^{n+1}(-1)^{n-k}\binom{n+1}{k}p(k) = 0.$$

This is simply Lagrange's interpolation formula written in a slightly changed form. We deduce from this and the binomial formula that

$$(a-1)^{n+1} = \sum_{k=0}^{n+1}(-1)^{n-k}\binom{n+1}{k}(p(k)-a^k).$$

Thus, if $|p(k)-a^k| < 1$ for all $0 \leq k \leq n+1$, then we must have

$$|a-1|^{n+1} < \sum_{k=0}^{n+1}\binom{n+1}{k} = 2^{n+1},$$

contradicting the fact that $a \geq 3$. This finishes the solution.

Remark. The identity

$$\sum_{k=0}^{n+1}(-1)^{n-k}\binom{n+1}{k}p(k) = 0$$

for polynomials of degree at most n is extremely useful. We proved it here as a consequence of Lagrange's interpolation formula, but it also follows from the theory of finite differences. The point is that $\Delta p(X) = p(X+1) - p(X)$ has degree smaller than $\deg p$, so that if one iterates Δ $\deg p + 1 \leq n+1$ times and applies it to p, one gets 0. But the evaluation at 0 of $\Delta^{n+1}p$ is

$$\sum_{k=0}^{n+1}(-1)^{n-k}\binom{n+1}{k}p(k),$$

as an immediate induction argument shows.

Example 1.64. *Let $n \geq 3$ and $f, g \in \mathbb{R}[X]$ be polynomials such that the points*

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

are vertices of a regular n-gon (anticlockwise). Then $\max(\deg f, \deg g) \geq n-1$.

Solution. It is enough to prove that the degree of $P(X) = f(X) + ig(X)$ is at least $n-1$. Clearly, we may assume that the regular n-gon has vertices $z, z^2, \ldots, z^n$ for $z = e^{\frac{2i\pi}{n}}$ (simply apply a translation and a homothety to reduce the general case to this one). So, it remains to prove that if a polynomial P satisfies $P(i) = z^i$ for all $1 \le i \le n$, then $\deg P \ge n-1$. Assume that this is not true. Using Lagrange's interpolation formula, we obtain

$$z^n = P(n) = \sum_{i=1}^{n-1} z^i \cdot \prod_{j \ne i} \frac{n-j}{i-j} = \sum_{i=1}^{n-1} \binom{n-1}{i-1} (-1)^{n-1-i} z^i.$$

By the binomial formula and cancelling similar terms we get $(1-z)^{n-1} = 0$, a contradiction.

Remark. Many other approaches may be considered. The most efficient is the method of finite differences, which yields

$$\Delta^{n-1} P(1) = \sum_{j=0}^{n-1} (-1)^j \binom{n-1}{j} P(n-j) = z(1-z)^{n-1} \ne 0.$$

Another very neat proof considers the polynomial $P(X+1) - zP(X)$. This has degree at most $n-2$, it is clearly nonzero and vanishes at $1, 2, \ldots, n-1$, a contradiction.

1.4.3 Polynomial with integer coefficients

Consider a polynomial $P(x) = a_n x^n + \cdots + a_1 x + a_0$ with integer coefficients. The difference $P(x) - P(y)$ can be written in the form

$$a_n(x^n - y^n) + \cdots + a_2(x^2 - y^2) + a_1(x - y),$$

in which all summands are multiples of polynomial $x - y$. This leads to the simple though important arithmetic property of polynomials from $\mathbb{Z}[x]$:

Theorem 1.10. *If P is a polynomial with integer coefficients, then $P(a) - P(b)$ is divisible by $a - b$ for any distinct integers a and b. In particular, all integer roots of P divide $P(0)$.*

There is a similar statement about rational roots of polynomial $P \in \mathbb{Z}[x]$.

Theorem 1.11. *If a rational number p/q $(p, q \in \mathbb{Z}, q \ne 0, \gcd(p,q) = 1)$ is a root of an integral polynomial $P(x) = a_n x^n + \cdots + a_1 x + a_0$, then $p \mid a_0$ and $q \mid a_n$.*

Proof. We have

$$q^n P\left(\frac{p}{q}\right) = a_n p^n + a_{n-1} p^{n-1} q + \cdots + a_0 q^n.$$

All summands but possibly the first are multiples of q, and all but possibly the last are multiples of p, hence $q \mid a_n p^n$ and $p \mid a_0 q^n$. □

Note that the polynomial that takes integer values at all integer points does not necessarily have integer coefficients, as seen on the polynomial $\frac{x(x-1)}{2}$. The result of the following problem is very important and goes back to Hilbert. This is why the polynomials $\frac{X(X-1)\cdots(X-n+1)}{n!}$ are also called **Hilbert polynomials.**

Theorem 1.12. *Let f be a polynomial with real coefficients. The following two assertions are equivalent:*

1° *For any integer n one has $f(n) \in \mathbb{Z}$;*

2° *There exist integers n and $a_0, a_1, a_2, \ldots, a_n$ such that*

$$f(X) = a_0 + a_1 X + a_2 \frac{X(X-1)}{2} + \cdots + a_n \frac{X(X-1)\cdots(X-n+1)}{n!}.$$

Proof. One implication follows from the fact that for all integers x and all $n \geq 1$, the number $x(x-1)\cdots(x-n+1)$ is a multiple of $n!$. This follows from the fact that $x(x-1)\cdots(x-n+1) = n!\binom{x}{n}$ if $x \geq 1$, while $x(x-1)\cdots(x-n+1) = (-1)^n \binom{-x+n-1}{n}$ if $x < 0$. For the interesting implication, the idea is that **any** polynomial f of degree n can be written

$$f(X) = a_0 + a_1 X + a_2 \frac{X(X-1)}{2} + \cdots + a_n \frac{X(X-1)\cdots(X-n+1)}{n!}$$

for suitable real numbers a_i and that the condition that f maps integers to integers forces all a_i be integers.

To prove the first claim, it is enough to prove that we can find (for all i) $a_0, \ldots, a_i$ such that $f(X) - a_0 - a_1 X - \cdots - a_i \frac{X(X-1)\cdots(X-i+1)}{i!}$ is a multiple of $X(X-1)\cdots(X-i)$. Choose $a_0 = f(0)$ and define inductively a_i by the relation

$$f(i) = a_0 + a_1 \binom{i}{1} + \cdots + a_{i-1} \binom{i}{i-1} + a_i.$$

By construction (or by an immediate induction), these a_i satisfy the desired conditions, since $f(X) - a_0 - a_1 X - \ldots - a_i \frac{X(X-1)\cdots(X-i+1)}{i!}$ is a multiple of $X(X-1)\cdots(X-i)$. But then $f(X) - a_0 - a_1 X - \cdots - a_i \frac{X(X-1)\cdots(X-n+1)}{n!}$ has degree at most n and is a multiple of a polynomial of degree $n+1$, so it has to be the zero polynomial. This establishes the existence of the a_i's. The construction we gave also shows that

$$a_i = f(i) - a_0 - a_1 \binom{i}{1} - \cdots - a_{i-1} \binom{i}{i-1},$$

which makes it clear that if all $f(i)$ are integers (actually, it is enough to have $f(i) \in \mathbb{Z}$ for $0 \leq i \leq n$), then so are the a_i's. The other implication is thus proved. □

Remark. 1° The fact that any polynomial of degree n can be written

$$f(X) = a_0 + a_1 X + a_2 \frac{X(X-1)}{2} + \cdots + a_n \frac{X(X-1)\cdots(X-n+1)}{n!}$$

for some real numbers a_i can also be proved using a linear algebra argument. Namely, the map $F : \mathbb{R}^{n+1} \to P_n$ (P_n being the set of polynomials with real coefficients and degree at most n) sending $(a_0, \ldots, a_n)$ to $a_0 + a_1 X + a_2 \frac{X(X-1)}{2} + \cdots + a_n \frac{X(X-1)\cdots(X-n+1)}{n!}$ is linear and clearly injective. Since the target and source are vector spaces of the same dimension, it has to be an isomorphism, thus surjective.

2° The desired relation can be written

$$f(X) = \sum_{i=0}^{n} a_i \binom{X}{i},$$

which immediately suggests the method of finite differences. Indeed, by this method, one obtains $a_k = \Delta^k(f)(0)$, where $\Delta(f)(X) = f(X+1) - f(X)$. This gives another proof, also classical, of the first part.

Theorem 1.13. *(Schur) Let $f \in \mathbb{Z}[X]$ be a non constant polynomial. Then the set of prime numbers dividing at least one non-zero number between the values $f(1)$, $f(2)$, …, $f(n)$, …, is infinite.*

Proof. First, suppose that $f(0) = 1$ and consider the numbers $f(n!)$. For sufficiently large n, they are non-zero integers. Moreover, $f(n!) \equiv 1 \pmod{n!}$ and so if we pick a prime divisor of each of the numbers $f(n!)$ we obtain the conclusion (since in particular any such prime divisor is greater than n). Now, if $f(0) = 1$, the conclusion is obvious. Suppose thus that $f(0) \neq 1$ and consider the polynomial $g(x) = \frac{f(xf(0))}{f(0)}$. Obviously, $g \in \mathbb{Z}[X]$ and $g(0) = 1$. Applying now the first part of the solution, we easily get the conclusion. □

We now present a number of illustrative examples.

Example 1.65. *Let $f \in \mathbb{Z}[X]$ be a non constant polynomial and n, k some positive integers. Then there exists a positive integer a such that each of the numbers $f(a), f(a+1), \ldots, f(a+n-1)$ has at least k distinct prime divisors.*

Solution. Let us consider an array of different prime numbers p_{ij}, with $i, j = 1, \ldots, k$ such that for some positive integers x_{ij} such that $f(x_{ij}) \equiv 0 \pmod{p_{ij}}$. We know that this is possible from Schur's Theorem. Now, using the Chinese remainder theorem we can find a positive integer a such that $ai - 1 \equiv x_{ij} \pmod{p_{ij}}$. It follows that each of the numbers $f(a)$, $f(a+1)$, …, $f(a+n-1)$ has at least k distinct prime divisors.

Example 1.66. *The polynomial $P \in \mathbb{Z}[x]$ takes the values ± 1 at three different integer points. Prove that it has no integer zeros.*

Solution. Suppose to the contrary, that a,b,c,d are integers with $P(a)$, $P(b)$, and $P(c)$ are in the set $\{-1,1\}$ and $P(d) = 0$. Then by Theorem 1.10 the integers $a-d$, $b-d$ and $c-d$ all divide 1, a contradiction.

Example 1.67. *Let $P(x)$ be a polynomial with integer coefficients. Prove that if $P(P(\cdots P(x)\cdots)) = x$ for some integer x (where P is iterated n times), then $P(P(x)) = x$.*

Solution. Consider the sequence given by $x_0 = x$ and $x_{k+1} = P(x_k)$ for $k \geq 0$. Assume $x_k = x_0$. As $d_i = x_{i+1} - x_i \mid P(x_{i+1}) - P(x_i) = x_{i+2} - x_{i+1} = d_{i+1}$ for all i, which together with $d_k = d_0$ implies $|d_0| = |d_1| = \ldots = |d_k|$.

Suppose that $d_1 = d_0 = d \neq 0$. Then $d_2 = d$ (otherwise $x_3 = x_1$ and x_0 will never occur in the sequence again). Similarly, $d_3 = d$ etc, and hence $x_k = x_0 + kd \neq x_0$ for all k, a contradiction. It follows that $d_1 = -d_0$, so $x_2 = x_0$.

Example 1.68. *Consider a polynomial P with integer coefficients and some distinct integers $a_1,a_2,\ldots,a_n$. Prove that if there exists a permutation σ of the set $\{1,2,\ldots,n\}$ such that $P(a_k) = a_{\sigma(k)}$, $k = 1,2,\ldots,n$, then $\sigma \circ \sigma$ is the identity.*

Solution. The statement is true if σ is the identity permutation e. If not, assume on the contrary that $\sigma \circ \sigma \neq e$. Hence, there is a $k \geq 3$ and k distinct integers $b_1,b_2,\ldots,b_k$ among $a_1,a_2,\ldots,a_n$ such that $P(b_l) = b_{l+l}$ for $l = 1,2,\ldots,k$ (here and henceforth, the indices are taken modulo k).

By Theorem 1.10, if P is a polynomial with integer coefficients, and u,v arbitrary distinct integers, then $u-v$ divides $P(u) - P(v)$. It follows that $b_l - b_{l+1}$ divides $P(b_l) - P(b_{l+1}) = b_{l+1} - b_{l+2}$ for $l = 1,2,\ldots,k$. Hence for each $l = 1,2,\ldots,k$ there is an integer q_l such that

$$b_{l+l} - b_{l+2} = q_l(b_l - b_{l+l}).$$

Multiplying the above equalities and simplifying, we get $q_1q_2\cdots q_k = 1$. Thus $q_l = \pm 1$ for $l = 1,2,\ldots,k$. Actually, no q_l can be -1, since otherwise the above relation yields $b_l = b_{l+2}$ and $b_1,b_2,\ldots,b_k$ are distinct by hypothesis. But $q_1 = q_2 = \ldots = q_k$ leads to a contradiction either. Indeed, in this case

$$b_1 - b_2 = b_2 - b_3 = \ldots = b_{k-1} - b_k = b_k - b_1,$$

and the sum of these equal numbers is 0. Then $b_1 = b_2 = \ldots = b_k$, and this is again impossible.

Example 1.69. *Suppose that the positive integer m and the real-valued polynomial $R(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_0$ are such that $R(x)$ is an integer divisible by m whenever x is an integer. Prove that $n!a_n$ is divisible by m.*

Solution. Apply Theorem 1.12 on the polynomial $\frac{1}{m}R(x)$. The leading coefficient of this polynomial is given by the expression $c_n + nc_{n-1} + \cdots + n!c_0$, and the property follows.

Example 1.70. *The polynomial $f(x) = x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n$ with integer non-zero coefficients has n distinct integer roots. Prove that if the roots are pairwise coprime, then a_{n-1} and a_n are coprime.*

Solution. Assume that $\gcd(a_{n-1}, a_n) \neq 1$. then both a_{n-1} and a_n are divisible by some prime p. Let the roots of the polynomial be $r_1, r_2, \ldots, r_n$. Then $r_1r_2, \ldots, r_n = (-1)^n a_n$. It follows that at least one of the roots, say r_1, is divisible by p. We also have

$$r_1r_2\cdots r_{n-1} + r_1r_3\cdots r_{n-1} + \cdots + r_2r_3\cdots r_n = (-1)^{n-1} \equiv 0 \pmod{p}.$$

All terms containing r_1 are divisible by p, hence $r_2r_3\cdots r_n$ is divisible by p. Hence $\gcd(r_1, r_2r_3\cdots r_n)$ is divisible by p contradicting the fact that the roots are pairwise coprime, and the conclusion follows.

Example 1.71. *Let $f_1, f_2, \ldots, f_k$ be nonconstant polynomials with integer coefficients. Prove that for infinitely many n all numbers $f_1(n), f_2(n), \ldots, f_k(n)$ are composite.*

Solution. Let $f_1, f_2, \ldots, f_k$ be the corresponding polynomials. By Schur's theorem, for any i there are infinitely many primes p that divide at least one of the numbers $f_i(1)$, $f_i(2)$, ... Thus, there are distinct primes $p_1, q_1, \ldots, p_k, q_k$ and integers $a_1, b_1, \ldots, a_k, b_k$ such that $f_i(a_i) \equiv 0 \pmod{p_i}$ and $f_i(b_i) \equiv 0 \pmod{q_i}$. By the Chinese Remainder Theorem, there are infinitely many n that satisfy $n \equiv a_i \pmod{p_i}, n \equiv b_i \pmod{q_i}$. For any such n we have $p_iq_i \mid f_i(n)$, so that $f_i(n)$ is composite for all i.

The following two problems are standard applications of the fact that $a - b$ divides $f(a) - f(b)$ if $f \in \mathbb{Z}[X]$ and $a, b \in \mathbb{Z}$ (see Theorem 1.10).

Example 1.72. *Let $f \in \mathbb{Z}[X]$ and let $n \geq 3$. Prove that there are no distinct integers $x_1, x_2, \ldots, x_n$ with $f(x_i) = x_{i-1}$, $i = 1, 2, \ldots, n$ (indices taken mod n).*

Solution. If such a polynomial f and integers x_i existed, $x_i - x_{i-1} = f(x_{i+1}) - f(x_i)$ would be divisible by $x_{i+1} - x_i$. In particular, $|x_i - x_{i-1}| \geq |x_{i+1} - x_i|$ for all i. This forces the numbers $|x_i - x_{i-1}|$ to be equal. This is however impossible. Indeed, if there is i such that $x_{i+1} - x_i$, $x_{i+2} - x_{i+1}$ have different signs, then $x_i = x_{i+2}$, which contradicts the hypothesis that x_i are all distinct. But such i has to exist, because $\sum_i (x_{i+1} - x_i) = 0$. This finishes the proof.

Example 1.73. *Let $f \in \mathbb{Z}[X]$ be a polynomial of degree $n \geq 2$. Prove that the polynomial $f(f(X)) - X$ has at most n integer zeros.*

Solution. Suppose that $x_1 < x_2 < \ldots < x_{n+1}$ are distinct integers such that $f(f(x_i)) = x_i$. Then $f(x_i)$ are also pairwise distinct and $f(x_i) - f(x_j)$ is a multiple of $x_i - x_j$. But $x_i - x_j = f(f(x_i)) - f(f(x_j))$ is also a multiple of $f(x_i) - f(x_j)$. Thus, we must have $|f(x_i) - f(x_j)| = |x_i - x_j|$. But then

$$f(x_{n+1}) - f(x_1) = \sum_{i=1}^{n} |f(x_{i+1}) - f(x_i)|,$$

which implies that all numbers $f(x_{i+1}) - f(x_i)$ have the same sign. Combined with the equality $|f(x_i) - f(x_{i+1})| = |x_i - x_{i+1}|$ this shows that either all numbers $f(x_i) + x_i$ are equal or that $f(x_i) - x_i$ are all equal. This is however impossible, as f has degree n.

Remark. Recently, a very similar problem featured in the IMO 2006: let $P(X)$ be a polynomial of degree $n > 1$ with integer coefficients and let k be a positive integer. Consider the polynomial

$$Q(X) = \underbrace{P(P(\cdots P(P}_{k \text{ times}}(X)))).$$

Prove that there are at most n integers such that $Q(t) = t$. It follows from Example 1.73 that any integral solution of the equation $Q(t) = t$ is a solution of the equation $P(P(t)) = t$, so this new problem is actually equivalent to the discussed one.

Example 1.74. *Find all integers $n > 1$ for which there is a polynomial $f \in \mathbb{Z}[X]$ with the property: for any integer k one has $f(k) \equiv 0 \pmod{n}$ or $f(k) \equiv 1 \pmod{n}$ and both these equations have solutions.*

Solution. The answer is: exactly the powers of a prime number. If n is a prime power, by Euler's theorem the polynomial $X^{\varphi(n)}$ is a solution.

Conversely, suppose there exists a polynomial f with the properties in the statement and that n has at least two different prime factors p, q. Changing f to $f(X - a)$ for a suitable a, we may assume that $f(0) \equiv 0 \pmod{n}$. Thus $f(0) \equiv 0 \pmod{q}$, which implies that for all $b \in \mathbb{Z}$ we also have $f(bq) \equiv 0 \pmod{q}$. So, we cannot have $f(bq) \equiv 1 \pmod{n}$, hence $f(bq) \equiv 0 \pmod{n}$.

In particular, $f(bq) \equiv 0 \pmod{p}$. But then for all $a \in \mathbb{Z}$ we also have $f(ap + bq) \equiv f(bq) \equiv 0 \pmod{p}$ and so $f(ap + bq) \equiv 0 \pmod{n}$. Since any integer $x \in \mathbb{Z}$ can be written $ap + bq$ for suitable a, b, it follows that the equation $f(x) \equiv 1 \pmod{n}$ has no solutions, a contradiction.

Example 1.75. *Find all polynomials f with integer coefficients which satisfy the property $f(n) \mid 2^n - 1$ for all positive integer n.*

Solution. Of course, if f is constant, then f has to be either 1 or -1 and these are solutions. So, assume that f is nonconstant. We may assume that the leading coefficient of f is positive. Take n such that $f(n) > 1$ and p a prime

factor of $f(n)$. Then $p \mid 2^n - 1$ while also $p \mid f(n+p)$ and $f(n+p) \mid 2^{n+p} - 1$. But then $p \mid 2^p - 1$, which is certainly impossible. So any such f is constant and the solutions are $1, -1$.

Here is a beautiful and rather tricky application which involves of ideas present in the proof of Hensel's lemma (see Lemma 3.1 in [91]).

Example 1.76. *Let p be a prime and let $f \in \mathbb{Z}[X]$ be a polynomial. If the values $f(0), f(1), \ldots, f(p^2-1)$ give distinct remainders when divided by p^2, prove that $f(0), f(1), \ldots, f(p^3-1)$ give distinct remainders when divided by p^3.*

Solution. Assume that $f(i) \equiv f(j) \pmod{p^3}$ for some i, j. Since $f(i) \equiv f(j) \pmod{p^2}$ and since f is injective mod p^2, we deduce that $i \equiv j \pmod{p^2}$, say $j = i + p^2 k$. It is enough to prove that $k \equiv 0 \pmod{p}$. Assume that this is not the case. We have

$$f(i) \equiv f(j) \equiv f(i + kp^2) \equiv f(i) + kp^2 f'(i) \pmod{p^3},$$

so p divides $kf'(i)$. Thus p divides $f'(i)$. But then

$$f(i + kp) \equiv f(i) + kpf'(i) \equiv f(i) \pmod{p^2},$$

which, combined with the hypothesis, yields $i + kp \equiv i \pmod{p^2}$, a contradiction. Thus $k \equiv 0 \pmod{p}$ and $i \equiv j \pmod{p^3}$. The conclusion follows.

We continue with a series of not so difficult problems.

Example 1.77. *Let $f \in \mathbb{Z}[X]$ be a nonconstant polynomial. Prove that the sequence $f(3^n) \pmod{n}$ is not bounded.*

Solution. Changing f with its opposite, we may assume that the leading coefficient of f is positive. So, given N, there exists m such that $f(3^m) > N$. Choose a prime $p > 2f(3^m)$ and observe that $f(3^{pm}) \equiv f(3^m) \pmod{p}$ by Fermat's little theorem. In particular, if $r = f(3^{mp}) \pmod{mp}$, then $r \equiv f(3^m) \pmod{p}$ and so $r \geq f(3^m) > N$, finishing the proof.

Example 1.78. *Is there a nonconstant polynomial $f \in \mathbb{Z}[X]$ and an integer $a > 1$ such that the numbers $f(a)$, $f(a^2)$, $f(a^3)$, ... are pairwise relatively prime?*

Solution. Assume that f is such a polynomial and a is as in the statement. Let $g = \gcd(a, f(a^k)) = \gcd(a, f(0))$. If $g > 1$, then g is a common factor of all $f(a^k)$. Thus $g = 1$, so a and $f(a^i)$ are relatively prime for all i. Choose an i with $|f(a^i)| > 1$ and choose $j = i + \varphi(|f(a^i)|)$, where φ is Euler's totient function. Then $f(a^i)$ divides $a^j - a^i$ by Euler's Theorem, so $f(a^i)$ divides $f(a^j) - f(a^i)$ and $f(a^i) | f(a^j)$. But this contradicts the fact that $\gcd(f(a^i), f(a^j)) = 1$ and shows that the answer to the problem is negative.

Example 1.79. *Find all polynomials f with integer coefficients such that there exists k such that for all primes p, $f(p)$ has at most k prime factors.*

Solution 1. Note that all polynomials of the form aX^m work, for obvious reasons. Let f be a solution of the problem and suppose f is not of this form. So we can write $f(X) = X^m g(X)$ for some polynomial g with integer coefficients such that $g(0) \neq 0$ and g is not constant. By Schur's theorem, there are infinitely many primes dividing at least one of the numbers $g(1), g(2), \ldots$. In particular, we can choose $p_1, p_2, \ldots, p_{k+1}$ distinct primes greater than $|g(0)|$ and we can choose positive integers $a_1, a_2, \ldots, a_{k+1}$ such that $g(a_i) \equiv 0 \pmod{p_i}$. Using the Chinese Remainder Theorem, we can find an integer a such that $a \equiv a_i \pmod{p_i}$ for all i.

Note that a is relatively prime to $p_1 p_2 \cdots p_{k+1}$ (otherwise some p_i would divide a, so $p_i \mid a_i$ and then $p_i \mid g(0)$, a contradiction). Thus, by Dirichlet's theorem, there exist infinitely many primes $p \equiv a \pmod{p_1 p_2 \cdots p_{k+1}}$. In particular, we can choose such a prime p with $f(p) \neq 0$. Since by construction $f(p)$ is a multiple of $p_1 p_2 \cdots p_{k+1}$, it follows that f is not a solution of the problem. The conclusion follows.

Solution 2. Note that all polynomials of the form $f(X) = aX^m$ work. Suppose $f(X) = X^m g(X)$ is such a polynomial which is not of this form. Then $g(X)$ is also such a polynomial. Thus we may assume that f is nonconstant and $f(0) \neq 0$. Let p be a prime not dividing $f(0)$, hence p does not divide $f(p)$. By Dirichlet's Theorem there are infinitely many primes q of the form $q = p + kf(p)^2$. Choose such a q with $|f(q)| > |f(p)|$. For such a q we have $f(q) \equiv f(p) \pmod{f(p)^2}$. Thus $f(q)$ is divisible by every prime factor of $f(p)$, with exactly the same multiplicities, and at least one additional prime factor. Iterating this construction, we can find a sequence of primes (p_n) for which $f(p_n)$ has at least n prime factors. Thus the only solutions where the ones already given.

Example 1.80. *Find all polynomials $f \in \mathbb{Z}[X]$ with the property that for any relatively prime integers m, n, the numbers $f(m), f(n)$ are also relatively prime.*

Solution 1. The solutions are the polynomials $\pm X^d$ for $d \geq 0$. Trivially, these are solutions of the problem. Consider now any nonconstant solution f and without loss of generality (change f into $-f$) we may assume that the leading coefficient of f is positive. Suppose that p is a large prime for which p does not divide $f(p)$. Then p and $p + f(p)$ are relatively prime and thus $f(p)$ and $f(p + f(p))$ are relatively prime. However, $f(p)$ divides $f(p + f(p))$. Thus necessarily $|f(p)| = 1$ or $f(p) = 0$. Since p was large, none of this happens (f is not constant). Thus, for p large enough we have $p \mid f(p)$, forcing $p \mid f(0)$. This implies that $f(0) = 0$ and so we can write $f(X) = Xg(X)$ for some polynomial g with integral coefficients. Of course, g satisfies the same property as f and has smaller degree. Repeating the argument with g or performing an obvious induction on the degree of f, we deduce that f is indeed of the form X^d for some d. This solves the problem.

Solution 2. Another proof can be based on the following preliminary result.

Lemma 1.2. *If $f \in \mathbb{Z}[X]$ is not of the form $\pm X^n$, then there exist different primes p,q such that $q \mid f(p)$.*

Proof of Lemma. Assuming the contrary, we may assume that the leading coefficient of f is positive. So, for all large enough p, $f(p) = p^{k_p}$ for some integer k_p. Since $k_p = \frac{\log f(p)}{\log p}$ converges to $\deg(f)$, it follows that $k_p = \deg(f)$ for all sufficiently large p and so $f(p) = p^{\deg(f)}$ for all sufficiently large p. The conclusion follows.

Coming back to the proof, choose a solution f of the problem and suppose that f is not of the form $\pm X^n$. Pick primes p,q as in the lemma. Then q divides $f(p)$ and $f(p+q)$ (since q divides $f(p+q) - f(p)$). But this is impossible, since $p, p+q$ are relatively prime and so $f(p)$ and $f(p+q)$ are relatively prime. The conclusion follows. □

Example 1.81. *Let f be a polynomial with integer coefficients and let $a_0 = 0$ and $a_n = f(a_{n-1})$ for all $n \geq 1$. Prove that $(a_n)_{n\geq 0}$ is a Mersenne sequence, that is $gcd(a_m, a_n) = a_{gcd(m,n)}$ for all positive integers m and n.*

Solution. Write f^d for the composite of f with itself d times. Pick any positive integers m,n and write $m = du, n = dv$ with $\gcd(u,v) = 1$ and observe that $a_n = f^n(0) = g^v(0)$ and $a_m = g^u(0)$, where $g = f^d$. Moreover, $a_d = g(0)$. So, it is enough to prove that for any g with integral coefficients and any $\gcd(u,v) = 1$ we have $\gcd(g^u(0), g^v(0)) = g(0)$. One may clearly notice that for any polynomial h with integer coefficients and any k we have $h(0) \mid h^k(0)$. Applying this to g already shows that $g(0)$ divides $\gcd(g^u(0), g^v(0))$. Conversely, let $x = \gcd(g^u(0), g^v(0))$. Applying the previous remark to $h = g^u$ and $h = g^v$, we obtain that for all $A, B \geq 1$ we have $x \mid g^{Au}(0)$ and $x \mid g^{Bv}(0)$. Taking A, B such that $Bv = Au + 1$, we get $x \mid g(g^{Au}(0))$ and $x \mid g^{Au}(0)$. Clearly, x divides $g(0)$ and the conclusion follows.

Example 1.82. *Find all integers k such that if an integral polynomial f satisfies $0 \leq f(0), f(1), \cdots, f(k+1) \leq k$, then $f(0) = f(1) = \cdots = f(k) = f(k+1)$.*

Solution. If $k \leq 2$ we can easily find examples, for instance $f(X) = X(2-X)$ for $k = 1$ and $f(X) = X(3-X)$ for $k = 2$. So, assume $k \geq 3$ and let f be a polynomial having integral coefficients with $0 \leq f(0), f(1), \ldots, f(k+1) \leq k$. As $f(k+1) - f(0)$ is between $-k$ and k and since it is a multiple of $k+1$, we must have $f(0) = f(k+1)$, hence

$$f(X) - f(0) = X(X - (k+1))g(X),$$

for some polynomial g, which clearly has integral coefficients (note that X divides $f(X) - f(0)$ and X is relatively prime to $X - (k+1)$). Thus, we have $f(0) + i(i-k-1)g(i)$ is between 0 and k for all $0 \leq i \leq k+1$. In particular

$$k \geq i(k+1-i)|g(i)|, \quad 0 \leq i \leq k+1.$$

However, $i(k+1-i) > k$, $2 \le i \le k-1$, hence $g(i) = 0$ for $2 \le i \le k-1$. In particular, we can write $g(X) = (X-2)\cdots(X-k+1)h(X)$, for some polynomial h, again with integral coefficients. But then

$$f(k) - f(0) = -k(k-2)!h(k), \quad f(1) - f(0) = (-1)^{k-1}k(k-2)!h(1).$$

This implies that $k(k-2)!|h(x)| \le k$ for $x \in \{1,k\}$, which clearly implies that $h(1) = h(k) = 0$, unless $k = 3$. Therefore, unless $k = 3$ we can definitely conclude that $f(0) = f(1) = \ldots = f(k+1)$ and so all $k \ge 4$ are solutions of the problem. For $k = 3$ we can actually have equality in all previous inequalities, hence we have the polynomial $f(X) = X(X-2)^2(4-X)$. Clearly, $k = 3$ is not a solution and the problem is solved.

Example 1.83. *Let n be a positive integer. What is the least degree of a monic polynomial f with integer coefficients such that $n \mid f(k)$ for any integer k?*

Solution. This is immediate. Indeed, by Theorem 1.12 we can write

$$\frac{f(X)}{n} = a_0 + a_1X + \cdots + a_d\frac{X(X-1)\cdots(X-d+1)}{d!},$$

where $d = \deg(f)$. Considering the leading coefficients in this equality shows that $d!$ is a multiple of n. On the other hand, if $d!$ is a multiple of n, then we can take $f(X) = X(X+1)\cdots(X+d-1)$. Thus the answer is: d is the smallest integer such that $d!$ is a multiple of n.

Example 1.84. *Let f be a polynomial with rational coefficients such that $f(n) \in \mathbb{Z}$ for all $n \in \mathbb{Z}$. Prove that for any integers m and n the number defined by the formula $lcm[1,2,\ldots,\deg(f)] \cdot \frac{f(m)-f(n)}{m-n}$ is an integer.*

Solution. Fix $m \ne n$ integers and let $d = m - n$ and $g(X) = f(n+X)$. Then g has rational coefficients, sends integers to integers and $\deg(f) = \deg(g)$. So, we need to prove that

$$\text{lcm}[1,2,\ldots,\deg(d)] \cdot \frac{g(d) - g(0)}{d}$$

is an integer. Using the result of problem 13, if $D = \deg(g)$, then there exist integers $a_0,\ldots,a_D$ such that

$$g(X) = \sum_{i=0}^{D} a_i\frac{X(X-1)\cdots(X-i+1)}{i!}.$$

So, it is enough to prove that for any $1 \le i \le D$ we have

$$\text{lcm}[1,2,\ldots,D] \cdot \frac{(d-1)(d-2)\cdots(d-i+1)}{i!} \in \mathbb{Z}.$$

But the last quantity can also be written as

$$\frac{(d-1)\cdots(d-i+1)}{(i-1)!}\cdot\frac{\operatorname{lcm}[1,2,\ldots,D]}{i},$$

making it clear that it is an integer. The conclusion follows.

Example 1.85. *Let f be a polynomial of degree d such that $f(\mathbb{Z})\subset\mathbb{Z}$ and for which $f(n)-f(m)$ is a multiple of $m-n$ for all $0\le m,n\le d$. Prove that $f(m)-f(n)$ is a multiple of $m-n$ for all integers m,n with $m\neq n$.*

Solution. The crucial point is the following consequence of the previous problem: if $L_k=\operatorname{lcm}(1,2,\ldots,k)$, then $m-n$ divides $L_k\left(\binom{m}{k}-\binom{n}{k}\right)$ for all integers $m\neq n$. Now, we will prove that if $m-n$ divides $f(m)-f(n)$ for all $0\le m\neq n\le d=\deg f$, then f is a linear combination with integer coefficients of the polynomials $L_k\binom{X}{k}$ for $0\le k\le d$. By the previous key point, this will be enough to conclude.

As $f(\mathbb{Z})\subset\mathbb{Z}$, by Exercise 1.78 there exist integers a_0, a_1, …, a_d such that

$$f(X)=a_0+a_1\binom{X}{1}+\cdots+a_d\binom{X}{d}.$$

It remains to prove that a_i is a multiple of L_i for all i. We prove this by induction, the case $i=0$ being clear (by definition $L_0=1$). Assume that $a_0,\ldots,a_{i-1}$ are multiples of $L_0,L_1,\ldots,L_{i-1}$ and fix $0\le j<i$. Then $j-i$ divides

$$f(i)-f(j)=\sum_{k=0}^{i}a_k\left(\binom{i}{k}-\binom{j}{k}\right)=a_i+\sum_{0\le k<i}a_k\left(\binom{i}{k}-\binom{j}{k}\right).$$

By the lemma and the inductive hypothesis, each of the numbers $a_k\left(\binom{i}{k}-\binom{j}{k}\right)$ with $0\le k<i$ is a multiple of $i-j$. We deduce that $i-j$ divides a_i and since $j<i$ was arbitrary, it follows that L_i divides a_i, which end the proof.

Chapter 2
Finite Sums and Products

2.1 How to use the sum symbol

In this section we discuss techniques of evaluating various special sums and products. special sums and products. A sum is simply repeated addition, and can be concisely expressed in **sigma notation** as follows:

$$\sum_{k=1}^{n} a_k = a_1 + a_2 + \cdots + a_k.$$

The expressions above and below the sigma are the bounds of the summation. Bounds can come in various forms; the only requirement is that the specify some (possibly empty) set over which the summation occurs. For example, the following are correct uses of sigma notation:

$$\sum_{i,j=1}^{n} a_{ij}, \qquad \sum_{1\le i<j\le n} a_{ij}, \qquad \sum_{\substack{1\le i,j\le 100 \\ ij=360}} a_{ij}, \qquad \sum_{p \text{ prime}} a_p.$$

Some important properties of sums are as follows:

$$\sum_{k=1}^{n} (a_k + b_k) = \left(\sum_{k=1}^{n} a_k\right) + \left(\sum_{k=1}^{n} b_k\right) \text{ (distributivity over addition)}$$

$$\sum_{k=1}^{n} (\alpha a_k) = \alpha \left(\sum_{k=1}^{n} a_k\right) \text{ (distributivity over multiplication by a constant)}$$

In the second example α must be a constant and cannot depend on k.

One important class of sums are **telescoping** sums. These are sums where almost all of the terms will cancel each other. There are two flavors of telescoping sums: **direct** and **indirect** telescoping sums.

2.2 Telescopic sums

A direct telescoping sum is one where there exists some sequence $\{x_k\}$ such that $a_k = x_{k+1} - x_k$ for $k = 1,2,\ldots,n$. In this case we may write

$$\sum_{k=1}^{n} a_k = \sum_{k=1}^{n} (x_{k+1} - x_k) = (x_2 - x_1) + \cdots + (x_{n+1} - x_n) = x_{n+1} - x_1.$$

An indirect telescoping sum is one where there exists some sequence $\{x_k\}$ such that $a_k = x_k - x_{k+1}$ for $k = 1,2,\ldots,n$. In this case we may write

$$\sum_{k=1}^{n} a_k = \sum_{k=1}^{n} (x_k - x_{k+1}) = (x_1 - x_2) + \cdots + (x_n - x_{n+1}) = x_1 - x_{n+1}.$$

A common goal of manipulating sums is to find a **closed form**, that is an expression equal to the sum that is free of sigma notation.

Example 2.1. *Find a closed form for* $\sum_{k=1}^{n} k(k+1)$.

Solution. We can expand $k(k+1) = k^2 + k$ and use formulas for sums of powers to compute a general form. However, there is an alternate method. We have $(k)(k+1)(k+2) - (k-1)(k)(k+1) = 3(k)(k+1)$, which gives $\sum_{k=1}^{n} k(k+1) = \frac{1}{3}\sum_{k=1}^{n}[(k)(k+1)(k+2) - (k-1)(k)(k+1)]$. This is a direct telescoping series; letting $x_k = (k-1)(k)(k+1)$, we have $\sum_{k=1}^{n}(x_{k+1} - x_k) = x_{n+1} - x_1 = n(n+1)(n+2) - 0$. Hence $\sum_{k=1}^{n} k(k+1) = \dfrac{n(n+1)(n+2)}{3}$.

Remark. We can use this identity, coupled with $\sum_{k=1}^{n} k = \dfrac{n(n+1)}{2}$, to find the closed form for $\sum_{k=1}^{n} k^2$.

Example 2.2. *Find a closed form for* $\sum_{k=1}^{n} k(k+1)(k+2)$.

Solution. Writing

$$k(k+1)(k+2) = [(k)(k+1)(k+2)(k+3) - (k-1)(k)(k+1)(k+2)]/4,$$

we obtain a direct telescoping sum analogous to that in Example 2.1. Writing $x_k = (k-1)(k)(k+1)(k+2)$, we have

$$\sum_{k=1}^{n} (x_{k+1} - x_k)/4 = (x_{n+1} - x_1)/4 = \frac{n(n+1)(n+2)(n+3)}{4}.$$

Example 2.3. *Let* $S = \sum_{k=1}^{n} k(k+1)\cdots(k+p)$. *We have*

$$k(k+1)\cdots(k+p) = \frac{1}{p+2}[k(k+1)\cdots(k+p+1) - (k-1)k\cdots(k+p)].$$

This is a telescoping series and we obtain

$$S = \frac{1}{p+2} n(n+1)\cdots(n+p)(n+p+1).$$

2.3 The sums $S_p(n) = \sum_{k=1}^{n} k^p$, $p = 0,1,2,\ldots$

We now consider sums of the form $S_p(n) = \sum_{k=1}^{n} k^p$, where p is a nonnegative integer. The closed forms for small p are

$$S_0(n) = n, \quad S_1(n) = \frac{n(n+1)}{2},$$
$$S_2(n) = \frac{n(n+1)(2n+1)}{6}, \quad S_3(n) = \left(\frac{n(n+1)}{2}\right)^2.$$

We show a more general relation for $S_p(n)$ in our next result.

Theorem 2.1. *The following relation holds:*

$$\binom{p+1}{1} S_p(n) + \cdots + \binom{p+1}{p} S_1(n) = (n+1)^{p+1} - n - 1.$$

Proof. By the binomial theorem,

$$(k+1)^{p+1} - k^{p+1} = \binom{p+1}{1} k^p + \binom{p+1}{2} k^{p-1} + \cdots + \binom{p+1}{p} k^1 + 1.$$

Summing this as k ranges from 1 to n gives

$$\sum_{k=1}^{n} (k+1)^{p+1} - k^{p+1}$$
$$= \binom{p+1}{1} \sum_{k=1}^{n} k^p + \binom{p+1}{2} \sum_{k=1}^{n} k^{p-1} + \cdots + \binom{p+1}{p} \sum_{l=1}^{n} k^1 + n.$$

The left-hand side of this sum reduces to $(n+1)^{p+1}-1$, while in the right-hand side we may replace our sums of powers of k with $S_p(n)$, hence

$$\begin{aligned}&(n+1)^{p+1}-1\\&=\binom{p+1}{1}S_p(n)+\binom{p+1}{2}S_{p-1}(n)+\cdots+\binom{p+1}{p}S_p(n)+n,\end{aligned}$$

which after a tiny bit of rearranging is exactly what we set out to prove. □

Using this method we can prove the following relations:

$$\begin{aligned}S_4(n)&=\frac{n(n+1)(2n+1)(3n^2+3n-1)}{30},\\S_5(n)&=\frac{n^2(n+1)^2(2n^2+2n-1)}{12},\\S_6(n)&=\frac{n(n+1)(2n+1)(3n^4+6n^3-3n+1)}{42}.\end{aligned}$$

Theorem 2.2. 1° *For all integers $p\geq 0$, $S_p(n)$ is a polynomial of degree $p+1$ in n with rational coefficients and leading coefficient $1/(p+1)$.*

2° *The coefficient of n^p is $\frac{1}{2}$, hence it does not depend on p.*

Proof. 1. We prove this by strong induction. We can verify that $S_0(n)=n$ satisfies the conditions above; this provides our base case. Suppose that for some $p\geq 1$ that $S_0(n), S_1(n), \ldots, S_{p-1}(n)$ satisfy the conditions above. We use the relation

$$(n+1)^{p+1}-1=\binom{p+1}{1}S_p(n)+\cdots+\binom{p+1}{p}S_p(n)+n$$

proved in Example 3. We rearrange this to write

$$S_p(n)=\frac{(n+1)^{p+1}-\binom{p+1}{2}S_{p-1}(n)-\cdots-\binom{p+1}{p}S_1(n)-n-1}{p+1}.$$

By our inductive hypotheses, the highest-degree term in the right-hand side is the $(n+1)^{p+1}$ term. Hence $S_p(n)$ is of degree $p+1$ in n. Similarly by our inductive hypothesis, the right-hand side has rational coefficients. Finally, as the only term of degree $p+1$ on the right-hand side is $(n+1)^{p+1}$, which expands to n^{p+1} plus lower-degree terms, the leading coefficient of $S_p(n)$ must be $1/\binom{p+1}{1}=1/(p+1)$ as desired.

2. Let a_p be the coefficient of n^p. Identifying the coefficient of n^p in the recursive relation, it follows $\binom{p+1}{1}=\binom{p+1}{1}a_p+\binom{p+1}{2}\frac{1}{p}$, hence $a_p=\frac{1}{2}$. □

2.4 The geometric sum

We will discuss now a very important class of sums.

Theorem 2.3. *For every complex number $a \neq 1$, the following formula holds:*

$$\sum_{k=0}^{n} a^k = \frac{1-a^{n+1}}{1-a}.$$

Proof. Let $S = \sum_{k=0}^{n} a^k$. Then we may write:

$$\begin{aligned} S &= 1 + a + a^2 + \cdots + a^n \\ -aS &= \quad -a - a^2 - \cdots - a^n - a^{n+1} \\ S - aS &= 1 - a^{n+1} \\ S &= \frac{1-a^{n+1}}{1-a} \end{aligned}$$

This ends the proof. □

Remark. For every complex number a with $|a| < 1$, we have $\sum_{k=1}^{\infty} a^k = \frac{1}{1-a}$.

Example 2.4. *Find a closed form for* $\sum_{k=0}^{n} ka^k$ *where* $a \neq 1$.

Solution. Let $S = \sum_{k=0}^{n} ka^k$. We rewrite S as

$$\begin{aligned} a + a^2 + a^3 + \cdots + a^n &= (a - a^{n+1})/(1-a) \\ a^2 + a^3 + \cdots + a^n &= (a^2 - a^{n+1})/(1-a) \\ a^3 + \cdots + a^n &= (a^3 - a^{n+1})/(1-a) \\ \ddots \quad = \qquad &\vdots \\ a^n &= (a^n - a^{n+1})/(1-a). \end{aligned}$$

Adding up the right-hand sides we get our desired sum. We have

$$\begin{aligned} S &= \frac{(a + a^2 + \cdots + a^n) - na^{n+1}}{1-a} \\ &= \frac{a - a^{n+1} - na^{n+1} + na^{n+2}}{(1-a)^2} \\ &= \frac{a - (n+1)a^{n+1} + na^{n+2}}{(1-a)^2}. \end{aligned}$$

Example 2.5. *Find a closed form for* $\sum_{k=0}^{n} k^2 a^k$ *where* $a \neq 1$.

Solution. Let $S = \sum_{k=0}^{n} k^2 a^k$. Then we may write

$$S - aS = \sum_{k=1}^{n} (k^2 - (k-1)^2) a^k = \sum_{k=1}^{n} (2k-1) a^k - n^2 a^{n+1}.$$

But this can be expressed in terms of sums we can already compute as

$$(1-a)S = 2\left(\frac{a-(n+1)a^{n+1}+na^{n+2}}{(1-a)^2}\right) - \left(\frac{a-a^{n+1}}{1-a}\right) - n^2 a^{n+1}.$$

We get

$$S = 2\frac{na^{n+2}-(n+1)a^{n+1}+a}{(a-1)^3} - \frac{a-a^{n+1}}{(a-1)^2} + n^2\frac{a^{n+1}}{a-1}.$$

2.5 Some interesting trigonometric sums

In this section we present a general trigonometric sum for which we provide three proofs, and a number of interesting consequences. The original material was published in [37], inspired by a proposed problem in [36].

Theorem 2.4. *For any real number* $a \in \mathbb{R} \setminus \{-1, 1\}$ *the following relation holds:*

$$\sum_{k=0}^{n-1} \frac{1}{a^2 - 2a\cos\frac{2k\pi}{n} + 1} = \frac{n(a^n+1)}{(a^2-1)(a^n-1)}. \tag{2.1}$$

Proof 1. Let $P \in \mathbb{R}[X]$ be a polynomial of degree $n-1$ with real coefficients denoted by $P = a_0 + a_1 X + \cdots + a_{n-1}X^{n-1}$. If $\alpha \in U_n$ is an nth root of unity, then we have

$$\begin{aligned}
|P(\alpha)|^2 &= P(\alpha)\cdot\overline{P(\alpha)} = P(\alpha)\cdot P(\overline{\alpha}) = P(\alpha)\cdot P\left(\frac{1}{\alpha}\right) \\
&= \left(a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}\right)\left(a_0 + \frac{a_1}{\alpha} + \cdots + a_{n-1}\frac{1}{\alpha^{n-1}}\right) \\
&= a_0^2 + a_1^2 + \cdots + a_{n-1}^2 + \sum_{k=1}^{n-1} A_k\alpha^k + \sum_{k=1}^{n-1} B_k\frac{1}{\alpha^k},
\end{aligned}$$

where the coefficients A_k, B_k, $k = 1, \ldots, n-1$ are different from zero. Using the relation (see [6, Proposition 3, page 46]) one gets

$$\sum_{\alpha\in U_n}\alpha^k=\begin{cases}n, & \text{if } n\mid k\\ 0, & \text{otherwise}\end{cases}$$

we get the following formula

$$\sum_{\alpha\in U_n}|P(\alpha)|^2=n\left(a_0^2+a_1^2+\cdots+a_{n-1}^2\right). \tag{2.2}$$

In order to prove (2.1) we consider the polynomial

$$P=1+aX+\cdots+a^{n-1}X^{n-1}=\frac{a^nX^n-1}{aX-1}.$$

Applying formula (2.2) it follows that

$$\sum_{\alpha\in U_n}|P(\alpha)|^2=n\left(1+a^2+\cdots+a^{2(n-1)}\right)=n\frac{a^{2n}-1}{a^2-1}. \tag{2.3}$$

On the other hand we have

$$\sum_{\alpha\in U_n}|P(\alpha)|^2=\left|\frac{a^n\alpha^n-1}{a\alpha-1}\right|^2=\frac{(a^n-1)^2}{(a\alpha-1)(a\overline{\alpha}-1)}=\frac{(a^n-1)^2}{a^2-2\mathrm{Re}\,\alpha\cdot a+1},$$

and the desired result follows. □

Proof 2. By the Poisson kernel formula one obtains

$$\frac{1-r^2}{1-2r\cos t+r^2}=\sum_{m=-\infty}^{\infty}r^{|m|}z^m,\ \text{where}\ |\,r\,|<1 \tag{2.4}$$

and $z=\cos t+i\sin t$. Applying this formula in the current problem one gets

$$\begin{aligned}\sum_{k=0}^{n-1}\frac{1-a^2}{1-2a\cos\frac{2k\pi}{n}+a^2}&=\sum_{k=0}^{n-1}\left(\sum_{m=-\infty}^{\infty}a^{|m|}e^{im\frac{2k\pi}{n}}\right)\\&=\sum_{m=-\infty}^{\infty}a^{|m|}\left(\sum_{k=0}^{n-1}\left(e^{\frac{2\pi im}{n}}\right)^k\right)\\&=\sum_{m\in\mathbb{Z}}na^{|m|}=n\sum_{j\in\mathbb{Z}}a^{n|j|}\\&=n\frac{1-a^{2n}}{(1-a^n)^2}=n\frac{1+a^n}{1-a^n},\end{aligned}$$

and the formula follows. □

Proof 3. Let $P\in\mathbb{C}[X]$ be a polynomial whose factorization is given by the formula $P=\prod_{k=0}^{n}\left(X^2+a_kX+b\right)$. We have the following relations

$$\frac{P'}{P}=\sum_{k=1}^{n}\frac{2X+a_k}{X^2+a_kX+b}=\frac{1}{X}\sum_{k=1}^{n}\frac{2X^2+a_kX+b-b}{X^2+a_kX+b}$$
$$=X\sum_{k=1}^{n}\frac{1}{X^2+a_kX+b}+\frac{n}{X}-\frac{b}{X}\sum_{k=1}^{n}\frac{1}{X^2+a_kX+b}$$
$$=\frac{X^2-b}{X}\sum_{k=1}^{n}\frac{1}{X^2+a_kX+b}+\frac{n}{X},$$

from where we can derive the formula

$$\frac{XP'-nP}{(X^2-b)P}=\sum_{k=1}^{n}\frac{1}{X^2+a_kX+b}. \tag{2.5}$$

For the polynomial

$$P=(X^n-1)^2=\prod_{k=0}^{n-1}\left(X^2-2X\cos\frac{2k\pi}{n}+1\right)$$

we have $P'=2nX^n(X^n-1)$, hence

$$\frac{XP'-nP}{(X^2-1)P}=\frac{2nX^{n-1}(X^n-1)-n(X^n-1)^2}{(X^2-1)(X^n-1)^2}=n\frac{X^n+1}{(X^2-1)(X^n-1)},$$

and the desired relation (2.4) follows from (2.5). □

In the case $n=7$ and $a\in(-1,1)$ one recovers Problem 49 in the Longlisted Problems of IMO 1988 (see [102, pp. 217]). We now present four examples inspired by the main result. The following problem was proposed in [36].

Example 2.6. *Evaluate the sum*

$$\sum_{k=0}^{n-1}\frac{1}{1+8\sin^2\left(\frac{k\pi}{n}\right)}. \tag{2.6}$$

Solution. Taking $a=2$ in (2.4) one obtains

$$\sum_{k=0}^{n-1}\frac{1}{4-4\cos\frac{2k\pi}{n}+1}=\frac{n(2^n+1)}{3(2^n-1)}, \tag{2.7}$$

which can be written as

$$\sum_{k=0}^{n-1}\frac{1}{1+8\sin^2\left(\frac{k\pi}{n}\right)}=\frac{n(2^n+1)}{3(2^n-1)}. \tag{2.8}$$

Example 2.7. *The following identity holds.*

$$\sum_{k=1}^{n-1} \frac{1}{\sin^2\left(\frac{k\pi}{n}\right)} = \frac{(n-1)(n+1)}{3}. \tag{2.9}$$

Solution. Indeed, the identity (2.1) can be written as

$$\sum_{k=1}^{n-1} \frac{1}{a^2 - 2a\cos\frac{2k\pi}{n} + 1} = \frac{n(a^n+1)}{(a^2-1)(a^n-1)} - \frac{1}{(a-1)^2}.$$

Taking the limit as $a \to 1$ on the right-hand side we get

$$\begin{aligned}
&\lim_{a\to 1}\left[\frac{n(a^n+1)}{(a^2-1)(a^n-1)} - \frac{1}{(a-1)^2}\right] \\
&= \frac{1}{2n}\lim_{a\to 1}\frac{(n-1)a^{n+1} - (n+1)a^n + (n+1)a - n + 1}{(a-1)^3} \\
&= \frac{1}{2n}\lim_{a\to 1}\frac{(n+1)(n-1)a^n - n(n+1)a^{n-1} + (n+1)}{3(a-1)^2} \\
&= \frac{1}{2n}\lim_{a\to 1}\frac{(n+1)(n-1)na^{n-2}(a-1)}{6(a-1)} = \frac{(n-1)(n+1)}{12}.
\end{aligned}$$

It follows that

$$\lim_{a\to 1}\sum_{k=1}^{n-1} \frac{1}{a^2 - 2a\cos\frac{2k\pi}{n} + 1} = \frac{(n-1)(n+1)}{12},$$

that is

$$\sum_{k=1}^{n-1} \frac{1}{4\sin^2\left(\frac{k\pi}{n}\right)} = \frac{(n-1)(n+1)}{12}.$$

Remark. 1° Using the symmetry

$$\sin^2\frac{k\pi}{n} = \sin^2\frac{(n-k)\pi}{n}, \quad k = 1,\ldots,n-1,$$

by the identity (2.9) one obtains the following results.

If $n = 2m+1$ is odd, then

$$\sum_{k=1}^{m} \frac{1}{\sin^2\left(\frac{k\pi}{2m+1}\right)} = \frac{2m(2m+2)}{6} = \frac{m(2m+2)}{3}.$$

Writing $1 = \sin^2 t + \cos^2 t$, this is equivalent to

$$\sum_{k=1}^{m} \operatorname{ctg}^2 \frac{k\pi}{2m+1} = \frac{m(2m-1)}{3}. \tag{2.10}$$

If $n = 2m$ is even, then one obtains

$$\sum_{k=1}^{\frac{n}{2}-1} \frac{1}{\sin^2\left(\frac{k\pi}{n}\right)} = \frac{1}{2}\left(\frac{n^2-1}{3} - 1\right) = \frac{n^2-4}{6}.$$

2° The identity (2.10) can also be proved by different means, as shown in [4, Page 147]. There the authors consider the trigonometric equation $\sin(2m+1)x = 0$, with the roots

$$\frac{\pi}{2m+1}, \frac{2\pi}{2m+1}, \ldots, \frac{m\pi}{2m+1}.$$

Writing $\sin(2m+1)x$ in terms of $\sin x$ and $\cos x$, we obtain

$$\begin{aligned}\sin(2m+1)x &= \binom{2m+1}{1}\cos^{2m} x \sin x - \binom{2m+1}{3}\cos^{2m-2} x \sin^3 x + \cdots \\ &= \sin^{2m+1} x \left(\binom{2m+1}{1}\operatorname{ctg}^{2m} x - \binom{2m+1}{3}\operatorname{ctg}^{2m-2} x + \cdots\right).\end{aligned}$$

Setting $x = \frac{k\pi}{2m+1}$, for $k = 1, \ldots, m$, and since $\sin^{2m+1} x \neq 0$ we obtain

$$\binom{2m+1}{1}\operatorname{ctg}^{2m} x - \binom{2m+1}{3}\operatorname{ctg}^{2m-2} x + \cdots = 0.$$

Substituting $y = \operatorname{ctg}^2 x$ this equation becomes

$$\binom{2m+1}{1} y^m - \binom{2m+1}{3} y^{m-1} + \cdots = 0,$$

which has the roots

$$\operatorname{ctg}^2 \frac{\pi}{2m+1}, \operatorname{ctg}^2 \frac{2\pi}{2m+1}, \ldots, \operatorname{ctg}^2 \frac{m\pi}{2m+1}.$$

By Vieta's relation between coefficients and roots one obtains

$$\sum_{k=1}^{m} \operatorname{ctg}^2 \frac{k\pi}{2m+1} = \frac{\binom{2m+1}{3}}{\binom{2m+1}{1}} = \frac{m(2m-1)}{3}.$$

Theorem 2.4 can also be used to prove other interesting identities.

Example 2.8. *If n is odd and $n \geq 3$, then*

$$\sum_{k=1}^{\frac{n-1}{2}} \frac{1}{\cos^2\left(\frac{k\pi}{n}\right)} = \frac{n^2-1}{2}. \tag{2.11}$$

If n is even and $n \geq 4$, then

$$\sum_{k=1}^{\frac{n}{2}-1} \frac{1}{\cos^2\left(\frac{k\pi}{n}\right)} = \frac{n^2-4}{6}. \tag{2.12}$$

Solution. In order to prove (2.11) note from (2.1) that we have

$$\sum_{k=0}^{n-1} \frac{1}{2+2\cos\frac{2k\pi}{n}} = \lim_{a\to -1} \frac{n(a^n+1)}{(a^2-1)(a^n-1)} \tag{2.13}$$

$$= \frac{n}{4} \lim_{a\to -1} \frac{a^n+1}{a+1} \tag{2.14}$$

$$= \frac{n^2}{4}. \tag{2.15}$$

That is

$$\sum_{k=0}^{n-1} \frac{1}{\cos^2\left(\frac{k\pi}{n}\right)} = n^2,$$

from where we obtain

$$\sum_{k=1}^{n-1} \frac{1}{\cos^2\left(\frac{k\pi}{n}\right)} = n^2 - 1.$$

From the symmetry

$$\cos^2\left(\frac{k\pi}{n}\right) = \cos^2\left(\frac{(n-k)\,\pi}{n}\right), \quad k = 1,\ldots,n-1, \tag{2.16}$$

one obtains the identity (2.11).

To prove (2.12) a few more steps are required. Again, by (2.1) one has the following

$$\begin{aligned}
\sum_{k=0,k\neq\frac{n}{2}}^{n-1}\frac{1}{2+2\cos\frac{2k\pi}{n}} &= \lim_{a\to-1}\left[\frac{n(a^n+1)}{(a^2-1)(a^n-1)}-\frac{1}{(a+1)^2}\right]\\
&= \lim_{t\to0}\left[\frac{n\left[(t-1)^n+1\right]}{t(t-2)\left[(t-1)^n-1\right]}-\frac{1}{t^2}\right]\\
&= -\frac{1}{2}\lim_{t\to0}\frac{n\left[(t-1)^n+1\right]t-(t-2)\left[(t-1)^n-1\right]}{t^2\left[(t-1)^n-1\right]}\\
&= -\frac{1}{2}\lim_{t\to0}\frac{nt\left[2-nt+\frac{n(n-1)}{2}t^2+t^3f(t)\right]}{t^2\left[-nt+\frac{n(n-1)}{2}t^2+t^3h(t)\right]}\\
&\quad -\frac{(t-2)\left(-nt+\frac{n(n-1)}{2}t^2-\frac{n(n-1)(n-2)}{6}t^3+t^4g(t)\right)}{t^2\left(-nt+\frac{n(n-1)}{2}t^2+t^3h(t)\right)}\\
&= -\frac{1}{2}\frac{\frac{n^2(n-1)}{2}-2\frac{n(n-1)(n-2)}{6}-\frac{n(n-1)}{2}}{-n}\\
&= \frac{n^2-1}{12},
\end{aligned}$$

since f, g, h are polynomials in t, so $f(0)$, $g(0)$ and $h(0)$ are finite. Hence,

$$\sum_{k=0,k\neq\frac{n}{2}}^{n-1}\frac{1}{2+2\cos\frac{2k\pi}{n}}=\frac{n^2-1}{3}.$$

By the symmetry of cosine formula (2.16) the identity (2.12) follows.

Remark. A direct proof of (2.12) can be obtained from (2.9) by using the symmetry relation

$$\cos^2\frac{k\pi}{n}=\sin^2\left(\frac{\pi}{2}-\frac{k\pi}{n}\right)=\sin^2\frac{(n-2k)\pi}{2n}=\sin^2\frac{\left(\frac{n}{2}-k\right)\pi}{n},\quad k=1,\ldots,\frac{n}{2}.$$

Example 2.9. *If $x\in\mathbb{R}$ and $|x|>1$, then*

$$\sum_{k=0}^{n-1}\frac{1}{x-\cos\frac{2k\pi}{n}}=\frac{2n\left(x+\sqrt{x^2-1}\right)\left[\left(x+\sqrt{x^2-1}\right)^n+1\right]}{\left[\left(x+\sqrt{x^2-1}\right)^2-1\right]\left[\left(x+\sqrt{x^2-1}\right)^n-1\right]}. \tag{2.17}$$

Solution. Indeed, we have

$$\sum_{k=0}^{n-1}\frac{1}{a^2-2a\cos\frac{2k\pi}{n}+1}=\frac{1}{2a}\sum_{k=0}^{n-1}\frac{1}{\frac{1}{2}\left(a+\frac{1}{a}\right)-\cos\frac{2k\pi}{n}}.$$

Letting $x = \frac{1}{2}\left(a + \frac{1}{a}\right)$, one has $a = x + \sqrt{x^2 - 1}$, and by identity (2.1) we get

$$\frac{1}{2a}\sum_{k=0}^{n-1}\frac{1}{x - \cos\frac{2k\pi}{n}} = \frac{n(a^n+1)}{(a^2-1)(a^n-1)},$$

which can be reduced to (2.17). In particular, for $x = 2$ one obtains

$$\sum_{k=0}^{n-1}\frac{1}{1+2\sin^2\left(\frac{k\pi}{n}\right)} = \frac{2n\left(2+\sqrt{3}\right)\left[\left(2+\sqrt{3}\right)^n+1\right]}{\left(3+3\sqrt{3}\right)\left[\left(2+\sqrt{3}\right)^n-1\right]}.$$

2.6 Finite products

We now move to products, where repeated multiplication can be concisely expressed in product notation (occasionally called **pi notation**) as

$$\prod_{k=1}^{n} a_k = a_1 a_2 a_3 \cdots a_n.$$

The indices on products can be written in different ways, just as with the indices on sums. (It is far less common to see unusual indices on products than on sums.) Some important properties of products are as follows:

$$\prod_{k=1}^{n}(a_k b_k) = \left(\prod_{k=1}^{n} a_k\right)\left(\prod_{k=1}^{n} b_k\right) \text{ (distribution over multiplication)}$$

$$\prod_{k=1}^{n}(\alpha a_k) = \alpha^n \prod_{k=1}^{n} a_k \text{ (distribution over multiplication by a constant)}$$

As with sums, an important class of products are telescoping products. There are two flavors of telescoping products, as before - direct and indirect telescoping products. A direct telescoping product is one where there exists a sequence x_k such that $a_k = \frac{x_{k+1}}{x_k}$ for $k = 1, 2, \ldots, n$, where we have

$$\prod_{k=1}^{n} a_k = \frac{x_{n+1}}{x_1}.$$

Analogously, an indirect telescoping product is one where there exists a sequence x_k such that $a_k = \frac{x_k}{x_{k+1}}$ for $k = 1, 2, \ldots, n$. In this case we may write

$$\prod_{k=1}^{n} a_k = \frac{x_1}{x_{n+1}}.$$

Example 2.10. *Compute the product*

$$\prod_{k=2}^{n} \frac{k^3-1}{k^3+1}.$$

Proof. We may write

$$\frac{k^3-1}{k^3+1} = \frac{(k-1)(k^2+k+1)}{(k+1)(k^2-k+1)},$$

hence we obtain

$$\begin{aligned}\prod_{k=2}^{n} \frac{k^3-1}{k^3+1} &= \prod_{k=2}^{n} \frac{(k-1)(k^2+k+1)}{(k+1)(k^2-k+1)} \\ &= \prod_{k=2}^{n} \frac{k-1}{k+1} \cdot \prod_{k=2}^{n} \frac{k^2+k+1}{k^2-k+1} \\ &= \frac{2}{n(n+1)} \cdot \prod_{k=2}^{n} \frac{k^2+k+1}{k^2-k+1}.\end{aligned}$$

In order to compute the last product, observe the following relation

$$\frac{k^2+k+1}{k^2-k+1} = \frac{k^2+k+1}{(k-1)^2+(k-1)+1},$$

therefore it is a direct telescopic product. Finally, we get

$$\prod_{k=2}^{n} \frac{k^3-1}{k^3+1} = \frac{2}{n(n+1)} \cdot \frac{n^2+n+1}{3} = \frac{2(n^2+n+1)}{3n(n+1)}.$$

Example 2.11. 1° *Prove that for every $n \geq 2$,*

$$\sum_{k=1}^{n-1} \frac{k}{(k+1)!} = 1 - \frac{1}{n!}$$

2° *Prove that for every positive integer $n \geq 3$, $n!$ can be written as sum of exact n of its distinct divisors.*

Solution. For the first part, note that for every $k \in \mathbb{N}^*$, we have the identity

$$\frac{k}{(k+1)!} = \frac{k+1-1}{(k+1)!} = \frac{1}{k!} - \frac{1}{(k+1)!}.$$

Using this, we get that

$$\sum_{k=1}^{n-1} \frac{k}{(k+1)!} = \sum_{k=1}^{n-1} \left(\frac{1}{k!} - \frac{1}{(k+1)!} \right).$$

The latter is a telescoping sum, where only the first and last terms survive. The desired conclusion follows immediately.

For the second part, note that multiplying by $n!$ the identity

$$\sum_{k=1}^{n-1} \frac{k}{(k+1)!} = 1 - \frac{1}{n!}$$

and re-arranging, we get that $1 + \sum_{k=1}^{n-1} \frac{n!}{(k+1)!} k = n!$. The conclusion follows by observing that for each $k \in \{1, 2, \ldots, n-1\}$, the expressions $\frac{n!}{(k+1)!} k$ are distinct divisors of $n!$.

Example 2.12. *Prove the inequality:*

$$\frac{2}{3} \cdot \frac{4}{5} \cdots \frac{2n}{2n+1} < \frac{3}{2n+3}$$

Solution. Regrettably, the product on the left side does not possess the property of being telescoping. Nevertheless, as we are tasked with proving an inequality rather than an equality, we may seek to identify a telescoping product that strictly exceeds the left-hand side while remaining less than or equal to the right-hand side.

Indeed, note that for every $k \in \mathbb{N}^*$ we have that $4k^2 + 4k + 1 < 4k^2 + 6k$, hence $(2k+1)^2 < 2k(2k+3)$. This implies that

$$\frac{2k}{2k+1} < \frac{2k+1}{2k+3}.$$

Now, the left hand side of our inequality can be written as $\prod_{k=1}^{n} \frac{2k}{2k+1}$, hence using the inequality above we get

$$\prod_{k=1}^{n} \frac{2k}{2k+1} < \prod_{k=1}^{n} \frac{2k+1}{2k+3} = \frac{3}{5} \cdot \frac{5}{7} \cdot \frac{7}{9} \cdots \frac{2n+1}{2n+3}.$$

The expression on the right is now a telescoping product and by cancelling terms we find that the product equals $\frac{3}{2n+3}$, as desired.

Chapter 3
Methods of Proof

3.1 Proof by contradiction

The method of argument by contradiction proves a statement in the following way: First, the statement is assumed to be false. Then, a sequence of logical deductions yields a conclusion that contradicts either the hypothesis (indirect method), or a fact known to be true (reductio ad absurdum). This contradiction implies that the original statement must be true. This is a method that Euclid loved, and you can find it applied in some of the most beautiful proofs from his Elements. Euclid's most famous proof is that of the infinitude of prime numbers.

Example 3.1 (Euclid). *There are infinitely many prime numbers.*

Solution. Assume, to the contrary, that only finitely many prime numbers exist. List them as $p_1 = 2, p_2 = 3, p_3 = 5, \ldots, p_n$. Then the number $N = p_1 p_2 \cdots p_n + 1$ is divisible by a prime p, yet is coprime to $p_1, p_2, \ldots, p_n$. Therefore, p does not belong to our list of all prime numbers, a contradiction. Hence the initial assumption was false, proving that there are infinitely many primes.

Example 3.2. *The number $\sqrt{2}$ is irrational.*

Solution. Assume that $\sqrt{2}$ is rational, that is $\sqrt{2} = \frac{m}{n}$, where m, n are positive integers. We may suppose that $\gcd(m,n) = 1$. By squaring, one obtains that $2n^2 = m^2$, hence $2 \mid n^2$, hence $n = 2n_1$, for some positive integer n_1. Replacing in $2n^2 = m^2$, we get $n_1^2 = 2m^2$, implying the numbers m, n are both divisible by 2, contradiction to $\gcd(m,n) = 1$.

Similarly, one can prove that if $d \in \mathbb{N}^*$ is not a perfect n-th power, then $\sqrt[n]{d}$ is not a rational number.

Example 3.3. *Let n be an odd positive integer and let $a_1, a_2, a_3, \ldots, a_n$ be a rearrangement of the numbers $1, 2, 3, \ldots, n$. Show that*

$$2 \mid (a_1 - 1)(a_2 - 2)(a_3 - 3) \cdots (a_n - n).$$

Solution. Assume, by contradiction, that $(a_1 - 1)(a_2 - 2)(a_3 - 3) \cdots (a_n - n)$ is odd. Then all factors $a_1 - 1, a_2 - 2, a_3 - 3, \ldots, a_n - n$ must be odd. Because n is odd, it follows their sum $(a_1 - 1) + (a_2 - 2) + (a_3 - 3) + \cdots + (a_n - n)$ is also odd. But, clearly, the sum is 0, a contradiction.

We continue with an example of Euler.

Example 3.4 (Euler). *Prove that there is no polynomial of degree at least 1 defined by $P(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$ with integer coefficients and with the property that $P(0), P(1), P(2), \ldots$, are all prime numbers.*

Solution. Assume the contrary and let $P(0) = p$ where, p is a prime. Then $a_0 = p$ and $P(kp)$ is divisible by p for all $k > 1$. Because we assumed that all these numbers are prime, it follows that $P(kp) = p$ for every $k > 1$. Hence, $P(x)$ takes the same value infinitely many times, a contradiction.

Example 3.5. *Suppose that a, b, c are rational numbers with $a + b\sqrt[3]{2} + c\sqrt[3]{4} = 0$. Show that $a = b = c = 0$.*

First solution. If, for example, $a = 0$, then we get that $b + c\sqrt[3]{2} = 0$ and since $\sqrt[3]{2}$ is irrational, we must have $c = b = 0$. One can similarly reach the same conclusion if $b = 0$ or $c = 0$. Suppose now that a, b, c are non-zero. Without losing generality we can assume that $a, b, c \in \mathbb{Z}$ are such that $\gcd(a, b, c) = 1$.

We know that

$$a + b\sqrt[3]{2} + c\sqrt[3]{4} = 0,$$

hence multiplying by $\sqrt[3]{2}$ we get

$$a\sqrt[3]{2} + b\sqrt[3]{4} + 2c = 0.$$

Eliminating $\sqrt[3]{4}$, one obtains

$$\sqrt[3]{2}(b^2 - ac) + ab - 2c^2 = 0.$$

As $\sqrt[3]{2}$ is not rational, we must have $b^2 - ac = 0$ and $ab - 2c^2 = 0$. Multiplying the last equality by c we get that $abc - 2c^3 = 0$, from where $b^3 - 2c^3 = 0$, which implies that $\sqrt[3]{2} = \frac{b}{c}$, a contradiction to the irrationality of $\sqrt[3]{2}$. Therefore, the only possibility is $a = b = c = 0$.

Second solution. If one of a, b or c is zero, then all of them must be zero.

Suppose that $abc \neq 0$. One can scale the such that $a, b, c \in \mathbb{Z}^*$ are such that $\gcd(a, b, c) = 1$. Denote by $x = a$, $y = b\sqrt[3]{2}$ and $z = c\sqrt[3]{2}$. From the given hypothesis, we have that $x + y + z = 0$. Moreover, using the identity (1.2)

$$x^3+y^3+z^3-3xyz=(x+y+z)(x^2+y^2+z^2-xy-yz-zx)=0,$$

and, replacing the substitutions,

$$a^3+2b^3+4c^3=3\cdot 2\cdot abc.$$

We observe that a must be even, so $2abc$ is divisible by 4, hence as $4\mid a^3+4c^3$ we deduce that b must be even. As, a,b are both even we know that $8\mid 2abc$ and as $8\mid a^3+2b^3$, we must have $8\mid 4c^3$, hence c is even. We obtained that 2 divides a, b and c, a contradiction with $\gcd(a,b,c)=1$.

3.2 The pigeonhole principle (or Dirichlet's box principle)

This principle is usually applied to problems in combinatorial set theory, combinatorial geometry, and number theory. In its intuitive form, it can be stated as follows.

Pigeonhole principle. *If $kn+1$ objects, where $k\geq 1$ is an integer, are distributed among n boxes, one of the boxes will contain at least $k+1$ objects.*

This is merely an observation, and it was Dirichlet who first used it to prove nontrivial mathematical results.

Example 3.6. *Consider a square of side-length 1 and 5 points inside. Prove that at least two points are situated at a distance $\leq \sqrt{2}/2$.*

Solution. Divide the square into four congruent squares by parallel lines to the sides, having each the length of sides $1/2$. At least two points are situated in the in a such square. But the maximum of possible distances in this small square is given by the diagonal, and it is $\sqrt{2}/2$.

Example 3.7. *From the set containing n arbitrary positive integers $\{a_1,a_2,\ldots,a_n\}$ we can select a subset in which the sum of all elements is divisible by n.*

Solution. Let us consider n subsets :

$$\{a_1\},\{a_1,a_2\},\ldots,\{a_1,a_2,\ldots,a_n\}.$$

First, calculate the sum of the elements in each subset and then the remainders after division by n. If some of these remainders is 0, we are done. If none, then according to the pigeonhole principle, among these n subsets there are at least two with equal remainders. Let $\{a_1,a_2,\ldots,a_r\}$ and $\{a_1,a_2,\ldots,a_s\}$, $r<s$, be two of such subsets. Then

$$a_1+a_2+\cdots+a_s-(a_1+a_2+\cdots+a_r)=a_{r+1}+a_{r+2}+\cdots+a_s$$

is divisible by n, and $\{a_{r+1},a_{r+2},\ldots,a_s\}$ is a subset we seek.

The following is a classical example in number theory that illustrates the existence of specific multiples with constrained decimal representations.

Example 3.8. *Prove that for any $n \in \mathbb{N}$, there exists a multiple of n whose decimal expansion consists only of the digits* 0 *and* 1.

Solution. If $n = 0$, the conclusion follows trivially, because 0 is a multiple of 0. We now suppose $n > 0$. For every $k \in \mathbb{N}^*$, write $a_k = \underbrace{\overline{111\ldots1}}_{k \text{ digits}}$. Looking at a_1, a_2, …, a_n, we distinguish the following two cases. If there exists a number $k \in \{1,2,\ldots,n\}$ such that $n \mid a_k$, then we are done. Otherwise, by the Pigeonhole Principle, the exists integers $1 \leq i < j \leq n$ such that a_i and a_j give the same remainder when divided by n. Then, their difference

$$a_j - a_i = \underbrace{\overline{11\ldots1}}_{j-i \text{ digits}} \underbrace{\overline{00\ldots0}}_{i \text{ digits}}$$

is a number with the desired property.

Let us give an easy example from the field of combinatorial geometry.

Example 3.9. *Consider a pentagon in the plane with vertices that have integer coordinates. Prove that the midpoint of at least one of its sides or diagonals also has integer coordinates.*

Solution. We denote by (x_i, y_i), where $i \in \{1,2,\ldots,5\}$ the coordinates of the vertices of the pentagon. Looking at the parities of these coordinates, we see that there are 4 possibilities, namely (even, even), (even, odd), (odd, even) and (odd, odd). By the Pigeonhole Principle, there are two vertices whose coordinates have the same party, i.e., there exists $1 \leq i < j \leq 5$ such that $x_i + x_j$ and $y_i + y_j$ are even integers.

Hence, the midpoint of the segment whose endpoints are (x_i, y_i) and (x_j, y_j) has integer coordinates $\left(\frac{x_i+x_j}{2}, \frac{y_i+y_j}{2}\right)$.

Another classical example of the same nature is the following.

Example 3.10. *Show that for any selection of $n+1$ positive integers, each less than or equal to $2n$, there are two numbers among them such that one divides the other.*

Solution. Write each of the $n+1$ integers $a_1, a_2, \ldots, a_{n+1}$ as a power of 2 times an odd integer. In other words, let $a_j = 2^{k_j} q_j$ for $j = 1,2,\ldots,n+1$, where k_j is a nonnegative integer and q_j is odd. The integers $q_1, q_2, \ldots, q_{n+1}$ are all odd positive integers less than $2n$. Because there are only n odd positive integers less than $2n$, it follows from the Pigeonhole Principle that two of the integers $q_1, q_2, \ldots, q_{n+1}$ must be equal. Therefore, there are distinct integers i and j such that $q_i = q_j$. Let q be the common value of q_i and q_j. Then, $a_i = 2^{k_i} q$ and $a_j = 2^{k_j} q$. It follows that if $k_i < k_j$, then a_i divides a_j; while if $k_i > k_j$, then a_j divides a_i.

Example 3.11. *A participant in a mathematics competition prepared intensively for 30 days leading up to the contest. During this period, the participant solved at least one test per day but no more than 45 tests in total. Prove that there exists a consecutive interval of days during which the participant solved exactly 14 tests.*

Solution. Let a_j be the number of tests solved on or before the j th day of the month. Then $a_1, a_2, \ldots, a_{30}$ is an increasing sequence of distinct positive integers, with $1 \leq a_j \leq 45$. Moreover, $a_1 + 14, a_2 + 14, \ldots, a_{30} + 14$ is also an increasing sequence of distinct positive integers, with $15 \leq a_j + 14 \leq 59$.

The 60 positive integers $a_1, a_2, \ldots, a_{30}, a_1 + 14, a_2 + 14, \ldots, a_{30} + 14$ are all less than or equal to 59 . Hence, by the pigeonhole principle two of these integers are equal. Because the integers $a_j, j = 1, 2, \ldots, 30$ are all distinct and the integers $a_j + 14, j = 1, 2, \ldots, 30$ are all distinct, there must be indices i and j with $a_i = a_j + 14$.

The previous example is taken from [226].

Example 3.12. *Prove that every set of* 10 *two-digit integer numbers has two disjoint subsets with the same sum of elements.*

Solution. Let S be the set of 10 numbers. It has $2^{10} - 2 = 1022$ subsets that differ from both S and the empty set. If $A \subset S$, the sum of elements of A cannot exceed $91 + 92 + \cdots + 99 = 855$. The numbers between 1 and 855, which are all possible sums, are the boxes. Since the number of objects exceeds the number of boxes, there will be two sums in the same box. Specifically, there will be two subsets with the same sum of elements. Deleting the common elements, we obtain two disjoint sets with the same sum of elements.

3.3 Mathematical induction

Mathematical induction is a technique used to prove that an infinite sequence of statements **that can be indexed by the natural numbers** is true. The importance of this phrase is paramount; induction can only be used when the statements to be proven correspond to the integers $\{1, 2, 3, \ldots\}$. Formally, mathematical induction is used to show that a sequence of statements

$$P_1, P_2, P_3, \ldots,$$

hold for all $n \geq n_0$, where n_0 is a positive integer. P_n can be any statement depending on n: for example, 'n is prime', 'n is bigger than 1', and 'I possess n cows' are all valid statements P_n. However, it would be rather strange were we able to successfully use induction on any but the second statement.

Mathematical induction comes in three flavors: weak induction, weak induction with step size s, and strong induction.

Each induction method has pros and cons:

- **Standard weak induction** is the simplest to use, but may not be strong enough;
- **Weak induction with step size** s is a slight extension of standard weak induction, useful for more complex problems.
- **Strong induction** is more complex than either weak induction, but is often hardest to apply.
- **Cauchy induction** also known as **lacunary induction**, is a lesser-known but powerful variant of induction.

All three types of induction arguments are split into two basic parts: the **base case** (or cases), and the **inductive step**. The base case is often a simple computation, whereas the theoretical arguments usually occur in the inductive step. In addition, the term **inductive hypothesis** appears in some texts. This may refer to two concepts. First, it may refer to the assumption we make that some P_i $(i \leq k)$ holds in our proof that P_{k+1} holds. Second, it may refer to the statement P_{k+1} itself - using this meaning, when we finish proving our inductive step, we may write that we have proven the inductive hypothesis.

3.3.1 Mathematical induction - weak form

Let P_n be a sequence of statements, and let n_0 be an integer. Suppose that the following hold:

1. P_{n_0} is true;
2. For $k \geq n_0$, P_k is true implies that P_{k+1} is true.

Then we may conclude that P_k is true for all $k \geq n_0$.

This is mathematical induction in its purest form. A simple example of the usefulness of this argument follows.

Example 3.13. *Show that for $n \geq 1$, we have*

$$1 + 2 + \cdots + n = \frac{n(n+1)}{2}.$$

Solution. Clearly, when $n = 1$, we have $1 = \frac{1(2)}{2}$. As $n_0 = 1$, this is our base case P_1. Suppose that P_n holds. We want to show that

$$1 + 2 + \cdots + n + (n+1) = \frac{(n+1)(n+2)}{2}.$$

Using our inductive hypothesis, we can write

$$1 + 2 + \cdots + n + (n+1) = (1 + 2 + \cdots + n) + n + 1 = \frac{n(n+1)}{2} + n + 1.$$

Dividing through by $n+1$, we obtain $\frac{n}{2}+1=\frac{n+2}{2}$, which is true. This completes our inductive step.

Let us now give an example which can be easily explained by the theory in the next chapter. Here we explain it using induction.

Example 3.14. *Show that if n people attend a party and each person shakes hands with every other person exactly once, then the total number of handshakes is* $\frac{n(n-1)}{2}$.

Solution. Now suppose that the statement is true for any party of k people, where $2 \leq k \leq n$. We need to show that the statement is true for any party of $n+1$ people. When the $(n+1)$-th person arrives to the party, they will shake hands with each of the n people who are already at the party.

By the inductive hypothesis, the n people who are already at the party have already shaken hands with each other a total of $\frac{n(n-1)}{2}$ times. Therefore, the $(n+1)$-th person shakes hands with n people, adding n handshakes to the total. This gives a total of

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

handshakes, completing the induction.

Example 3.15. 1° *Prove that for any positive integer n,*

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

2° *Show that for all integers* $n \geq 3$ *the equation*

$$\frac{1}{x_1}+\frac{1}{x_2}+\cdots+\frac{1}{x_n}=1,$$

is solvable in distinct positive integers.

Solution. 1°. Let P_n be the following statement:

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

We prove that the statement P_n is true for all $n \in \mathbb{N}^*$ using (the weak form of) induction on n. P_1 holds trivially, as on the left we have the empty sum and on the right $1-\frac{1}{1!}=0$. Similarly, it is easy to check that P_2 holds. Suppose P_m is true. We are trying to prove P_{m+1}. Using the validity of P_m, we get that the sum appearing in P_{m+1} is equal to

$$\sum_{k=1}^{m}\frac{k}{(k+1)!}=1-\frac{1}{m!}+\frac{m}{(m+1)!}=1-\frac{m+1-m}{(m+1)!}=1-\frac{1}{(m+1)}.$$

Hence P_{m+1} is true and the induction is complete.

2°. From the first part, we know that

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

so for every $n \geq 3$ one can choose $x_1 = 2!$, $x_2 = \frac{3!}{2} = 3$, $x_3 = \frac{4!}{3} = 8$, …, $x_{n-1} = \frac{n!}{n-1}$ and $x_n = n!$. The terms x_1, x_2, …, x_n are in strictly increasing order.

3.3.2 *Mathematical induction with step size s*

Let P_n be a sequence of statements, let n_0 be an integer, and let $s \geq 2$ be an integer. Suppose that the following hold:

1. $P_{n_0}, P_{n_0+1}, P_{n_0+2}, \cdots, P_{n_0+s-1}$ are true;
2. For $k \geq n_0$, P_k is true implies that P_{k+s} is true.

Then we may conclude that P_k is true for all $k \geq n_0$.

Mathematical induction with step size s is used in a variety of problems; a common example is to show that an expression is an integer for all values of n (or divisibility, which is nearly equivalent). Many other interesting problems also require induction with step size s, as the three presented below.

Example 3.16. *Show that a square may be divided into $n \geq 6$ smaller squares.*

Solution. We will use $n_0 = 6$ and $s = 3$. We first prove our base cases.

We first divide a square into 9 smaller squares, then merge 4 of them to obtain a division into 6 squares, proving P_6.

We divide a square into 4 smaller squares, dividing one of them into 4 still smaller squares to obtain a division into 7 squares. This proves P_7.

We then divide a square into 16 smaller squares, then merge 9 of them to obtain a division into 8 squares, effectively proving P_9.

Using the base cases P_6, P_7, P_8, we show the inductive step P_k implies P_{k+3}.

Let $k \geq 6$, and suppose we may divide a square into k smaller squares. Let S be one of these squares. If we divide S into 4 smaller squares, then we deleted 1 square, and added 4 squares, for a net increase of 3 squares. Hence we have a division of the square into $k+3$ smaller squares. This completes our inductive step. We may conclude that P_k holds for all $k \geq 6$.

Example 3.17. *Show that any $n \geq 8$ can be written as a sum of 3's and 5's.*

Solution. We will use $n_0 = 8$ and $s = 3$. We first prove our base cases.

We may write $8 = 3+5, 9 = 3+3+3, 10 = 5+5$. These establish our base cases P_8, P_9, P_{10}. We proceed to the inductive step, that P_k implies P_{k+3}.

Suppose that k may be written as a sum of 3's and 5's. Then by adding another 3 to this summation, we may obtain a sequence of 3's and 5's which sum to $k+3$. Hence $k+3$ can be written as a sum of 3's and 5's. This completes our inductive step. We may thus conclude that P_k holds for all $k \geq 8$.

Example 3.18. *Let α be any real number such that $\alpha + \dfrac{1}{\alpha}$ is an integer. Prove that $\alpha^n + \dfrac{1}{\alpha^n}$ is an integer for all $n \in \mathbb{Z}$.*

Solution. We may assume that $n \geq 0$. Let $E_n = \alpha^n + \dfrac{1}{\alpha^n}$. We want to prove that E_n is an integer for any $n \geq 0$. We note that $E_0 = 2 \in \mathbb{Z}$, $E_1 = \alpha + \dfrac{1}{\alpha} \in \mathbb{Z}$, $E_2 = \alpha^2 + \dfrac{1}{\alpha^2} = \left(\alpha + \dfrac{1}{\alpha}\right)^2 - 2 \in \mathbb{Z}$. The following relation holds:

$$E_{n+2} = \left(\alpha + \frac{1}{\alpha}\right) E_{n+1} - E_n, \ \forall n \geq 0.$$

Using induction with step $s = 2$, we get that E_n is an integer, for any $n \geq 0$.

In this example, taken from [226] we demonstrate how mathematical induction can be applied to solve paving problems in combinatorics. Such problems often involve recursive structures and careful reasoning to ensure that the paving is possible under specific constraints. The following example involves paving a modified chessboard using a particular type of tile.

Example 3.19. *Let n be a natural number. Show that any $2^n \times 2^n$ checkerboard with one square removed can be tiled using pieces of size 2×2 with one square removed (L-shaped trominoes), where each tile covers exactly three squares.*

Solution. We will prove the statement by induction on n. For every $n \in \mathbb{N}^*$, let P_n be the statement that such a covering exists for every $2^n \times 2^n$ board, with one square removed.

P_1 is obviously true, as an 2×2 board with one square removed is exactly a trominoe. Suppose now that P_n is true. Given an $2^{n+1} \times 2^{n+1}$ board with one square removed, we first divide the board in 4 equal squares of dimension $2^n \times 2^n$. Write A_1, A_2, A_3 and A_4 for these squares. The missing 1×1 square will be in one of these four squares, so we can assume without losing generality that it is missing from A_1. Now, we place the first L-shaped trominoe in the middle 2×2 square, such that the 3 squares fall in A_2, A_3 and A_4, respectively.

Now, each of the squares A_1, A_2, A_3 and A_4 are squares of size $2^n \times 2^n$ with one missing square. Hence, using the inductive hypothesis P_n, these can be covered by L-shaped trominoes, hence so does the entire $2^{n+1} \times 2^{n+1}$ square. The induction is now complete.

The following example demonstrates an important concept: the existence of a Gray code for subsets of a finite set. A Gray code is a sequence of binary strings or subsets where consecutive elements differ by exactly one element. This concept has significant applications in computer science, particularly in coding theory.

Example 3.20. *Show that for every $n \in \mathbb{N}^*$ and every set A such that $|A| = n$, there exists a numbering of all subsets $A_1, \ldots, A_{2^n}$ of A such that $\forall 1 \leq i \leq 2^n - 1$ we have*

$$|\,(A_i \setminus A_{i+1}) \cup (A_{i+1} \setminus A_i)\,| = 1.$$

Solution. We will prove the result by induction on $n \in \mathbb{N}^*$. Let P_n be the statement that there exists a numbering with the desired property for every set with n elements. P_1 is obviously true, as there are only two subsets of any one-element set. These are $\emptyset$ and the entire set.

Suppose now that P_n is true for some n and let A be a set with $n+1$ elements, one of them being $a \in A$. By the induction hypothesis, since $|A \setminus \{a\}| = n$, the 2^n subsets of $A \setminus \{a\}$ can be numbered $A_1, \ldots, A_{2^n}$ such that $|\,(A_i \setminus A_{i+1}) \cup (A_{i+1} \setminus A_i)\,| = 1$. These 2^n sets are also subsets of A.

Now, for every $1 \leq i \leq 2^n$, define the set

$$A_{2^n+i} = A_{2^n+1-i} \cup \{a\}.$$

The sets $A_1, A_2, \ldots, A_{2^{n+1}}$ are all subsets of A and we leave it as an exercise for the reader to complete the induction by showing that the last $2^n + 1$ sets in the numbering also satisfied the required condition.

By now, we hope the reader is convinced that mathematical induction is a powerful and versatile tool, capable of solving problems across various areas of mathematics. To further illustrate its broad applicability, we present the following two examples from the field of combinatorial geometry.

Example 3.21. *A finite number of lines divide the plane into regions. Prove that these regions can be colored with two colors such that any two adjacent regions have different colors.*

Solution. Let us write P_n for the statement that the regions formed by any n lines can be colored with, say, red or blue such that any two adjacent regions have different colors.

P_1 is obviously true, as we have only two regions and we can color one red and one blue. Assume P_n is true and, to prove that P_n implies P_{n+1} let us consider $l_1, l_2, \ldots l_n, l_{n+1}$ distinct lines in the plane. First, we ignore the line l_{n+1} and we look at all the regions formed when the lines $l_1, l_2, \ldots, l_n$ divide the plane. By the induction hypothesis P_n, we can color these regions such that no two adjacent regions have the same color.

Consider such a coloring and, on top of it, add the line l_{n+1}. New regions are formed by this line, on the plane which is already colored. On one side

of the line l_{n+1}, we will retain the same colors of the regions. On the other side of the line l_{n+1}, we will change the colors of the region, that is, if some region was red, we color it blue and vice-versa. It is easy to see that this coloring satisfies the requirements, so the induction is complete.

The next example is closely connected to an important result in combinatorial geometry, the Sylvester–Gallai theorem (see [74]). In fact, the inductive step in the solution of our example below is equivalent to the statement of this theorem. The result explores the relationship between points and lines in the plane. This example is more challenging than the previous ones.

Example 3.22. *Prove that for any $n \geq 3$ points in the plane, not all collinear, they determine at least n distinct lines.*

Solution. We first prove the following result, which will be used in the inductive step.

Lemma 3.1 (Sylvester-Gallai). *For every integer $n \geq 2$ and any n points in the plane, either all lie on a line, or there is a line which contains exactly 2 of these points.*

Proof. We here present a proof by Kelly [152]. Let us suppose that the n points are not all collinear and denote by $\mathcal{P}$ this set of points. Let $S = \{(l, P) \mid l \text{ is a line determined by two points in } \mathcal{P} \text{ and } P \in \mathcal{P}\}$. Since S is a finite set, there is a pair (l, P) such that the distance $d(l, P)$ is minimal among all distances between the pairs consisting of lines and points from S.

Assume that l contains at least three points from $\mathcal{P}$. At least two of these are on the same side of P', the perpendicular projection of P on l. Call them B and C, with B being closest to P' (and possibly coinciding with it). Draw the connecting line m passing through P and C, and the perpendicular from B to B' on m. Then BB' is shorter than PP'. This follows from the fact that $PP'C$ and $BB'C$ are similar triangles, one contained inside the other. This contradicts the minimality of $d(l, P)$, hence l contains exactly two points from $\mathcal{P}$. □

Going back to the solution of our problem, let P_n be the statement that any n distinct points in the plane, not all collinear, determine at least n distinct lines. Note that P_3 is true, as three such points determine a triangle and of course that there are exactly 3 lines (supporting the sides of the triangle) determined by them.

Let us suppose that P_n is true for some n. Consider a set of $n + 1$ points in the plane, not all collinear. By the lemma above, let l be a line that passes through exactly 2 points, denoted by A and B. Now, ignoring the point A, there are at least n lines determined by the n points in the set, without the point A. These lines are different from l, because if one of them would be l, then l would contain A and two other distinct points, which is not possible. Hence, together with l, the $n + 1$ points must determine at least $n + 1$ lines, so P_{n+1} is true and the induction is complete.

3.3.3 Mathematical induction - strong form

Let P_n be a sequence of statements, and let n_0 be an integer. Suppose that the following hold:

1. P_{n_0} is true;
2. For $k \geq n_0$, P_m being true for every m with $n_0 \leq m \leq k$ implies P_{k+1} is true.

Then we may conclude that P_k is true for all $k \geq n_0$.

Weak induction is often simpler and more intuitive, but sometimes a statement can only be proven by strong induction. As we saw in induction with step s, sometimes the inductive step requires more than just the previous case. If the inductive step length required is not known, strong induction can be used to assume that all the previous cases are true.

A classical and illustrative example is the following.

Example 3.23. *Prove that every positive integer can be expressed as a sum of distinct powers of* 2.

Solution. We will prove this statement by strong induction on the positive integer n. For the base case, $n = 1$, we see that 1 can be expressed as 2^0.

Now suppose that the statement is true for all positive integers less than or equal to n. We need to show that the statement is true for $n + 1$. Let 2^k be the largest power of 2 that is less than or equal to $n + 1$. Then, $n + 1 - 2^k$ is a positive integer less than or equal to k.

By the inductive hypothesis, $n + 1 - 2^k$ can be expressed as a sum of distinct powers of 2. Then, adding 2^k to this expression gives a representation of $n + 1$ as a sum of distinct powers of 2. Therefore, the statement is true for $n + 1$, and the proof is complete.

Oftentimes strong induction is useful not because it is the only way to solve a problem, but because it makes a solution very elegant. This is the case in the following problem.

Example 3.24. *Show that for all $k \geq 3$, and for any convex k-gon, we may draw segments that connect two vertices which do not lie on the same edge and obtain a division of the polygon into triangles whose vertices are among those of the polygon. (this is called a* ***triangulation*** *of a polygon.)*

Solution. We have $n_0 = 3$. P_3 is obviously true; we do not need to draw any segments to triangulate a triangle. We proceed to our inductive step.

Let $k \geq 3$, and suppose that $P_3, P_4, \cdots, P_k$ are true. Draw some $(k+1)$-gon $\mathcal{P}$ and some segment S between two vertices of $\mathcal{P}$ that do not lie on the same edge. This edge divides $\mathcal{P}$ into two polygons $\mathcal{Q}_1$ and $\mathcal{Q}_2$. As the total number of vertices in $\mathcal{Q}_1$ and $\mathcal{Q}_2$ is $k + 3$ (both of the endpoints of S are shared by $\mathcal{Q}_1$ and $\mathcal{Q}_2$), but as both have at least 3 vertices, it follows that both $\mathcal{Q}_1$ and $\mathcal{Q}_2$ have at most k vertices. Hence by our inductive hypothesis,

they can both be triangulated. But then constructing the triangulations of $\mathcal{Q}_1$ and $\mathcal{Q}_2$, together with the segment S, provides a triangulation of $\mathcal{P}$. This proves our inductive step. It follows that P_k is true for all $k \geq 3$.

The final list of examples is a selection of competition problems from the wonderful book [9]. We recommend this resource to the reader interested in learning about the use of induction in many areas of mathematics, including topics that are not discussed in an competition problems-oriented book.

Example 3.25. *Let n be a positive integer. Does n^2 have more positive divisors of the form $4k-1$ or of the form $4k+1$?*

Solution. Let $A(n)$ be the number of divisors of n^2 which are of the form $4k-1$ and let $B(n)$ be the number of divisors of the form $4k+1$.

After exploring a few values of $A(n)$, $B(n)$ for $n = 1$, 2, 3, we decide to prove by strong induction that $A(n) < B(n)$.

First note that if $n = 2^k$ is a power of 2, then we have $A(n) = 0 < B(n) = 1$.

If p is a prime such that $p \nmid n$ and $p = 4m+1$, then every divisor of $(p^a n)^2 = p^{2a}n^2$ of the form $4k-1$ is a power of p times a divisor of n^2 of the same form. Hence $A(p^a n) = (2a+1)A(n)$. By the same reasoning, $B(p^a n) = (2a+1)B(n)$. So, in this case, $A(n) < B(n)$ if and only if $A(p^a n) < B(p^a n)$.

Now, let $p \nmid n$ be a prime of the form $p = 4m-1$. Then every divisor of $(p^a n)^2 = p^{2a}n^2$ of the form $4k-1$ is either p^{2b} times a divisor of n^2 of the form $4t-1$, or p^{2b-1} times a divisor of n^2 of the form $4k+1$. More precisely, $A(p^a n) = (a+1)A(n) + aB(n)$. With a similar argument, one can show that $B(p^a n) = (a+1)B(n) + aA(n)$. Now, if $A(n) < B(n)$ then, $A(p^a n) < B(p^a n)$.

Let us now proceed to the proof. Using strong induction, assume that $A(k) < B(k)$ for all $1 \leq k \leq n-1$. We are trying to prove that $A(n) < B(n)$. If n is a power of 2, then the conclusion holds by the remark at the beginning. Otherwise, let p be an odd prime factor of n and let a be the highest power of p that divides n. Using the (strong) induction hypothesis, we have that $A(n/p^a) < B(n/p^a)$. As $p \nmid (n/p^a)$, the inequalities in the previous paragraph imply that $A(n) < B(n)$ and the induction is complete.

The result below is commonly known as the Cauchy-Davenport theorem.

Example 3.26. *Let $p \geq 3$ be a prime number and denote by $\mathbb{F}_p$ the field with p elements. Show that for any two non-empty subsets $A, B \subseteq \mathbb{F}_p$, we have*

$$|A+B| \geq \min(|A| + |B| - 1, p),$$

where $A + B = \{a+b \mid a \in A, b \in B\}$.

Solution. The proof we present uses strong induction on $|A|$. When $|A| = 1$, note that $|A+B| = |B|$, so there is nothing to prove.

Suppose the inequality holds for any set A' with at most $k-1$ elements, where $k \geq 2$. Suppose now that $|A| = k > 1$. Without losing generality, we

can assume that $0 \in A$. This is because we can translate the set A with $-a$, if a is some fixed element in A. Such a translation keeps both $|A|$ and $|A+B|$ unchanged, hence it does not affect the statement of the problem.

As $k \geq 2$, let $x \neq 0$ be an element from A. Note that if $B = \emptyset$ or $B = \mathbb{F}_p$ there is nothing to prove, so we can assume that $q \leq |B| < p$. Thus, there is $n \in \mathbb{F}_p$ such that $nx \in B$ but $(n+1)x \notin B$. Translating B with $-nx$, we get that $0 \in B$ but $x \notin B$.

First, we notice that $A \cup B + A \cap B \subseteq A + B$ holds trivially. This gives the inequality $|A+B| \geq |A \cup B + A \cap B|$.

Now $A \cap B$ is a strict subset of A, because $0 \in A \cap B$ but $x \in A \setminus B$. Hence, we can use the induction hypothesis to deduce that

$$|A \cup B + A \cap B| \geq \min(|A \cap B| + |A \cup B| - 1, p).$$

It is easy to prove that $|A| + |B| = |A \cup B| + |A \cap B|$, from where we get

$$|A+B| \geq |A \cup B + A \cap B| \geq \min(|A| + |B| - 1, p),$$

completing the induction.

Example 3.27. *Show that for every integer $n \geq 2$, we can choose distinct numbers $a_1, a_2, \ldots, a_n \in \{1,2,\ldots,n\}$ such that none of the numbers a_1, $a_1 + a_2$, …, $a_1 + a_2 + \cdots + a_{n-1}$ is a perfect square.*

Solution. If $n = 2$, we can choose $a_1 = 2$, $a_2 = 1$. For $n = 3$ we choose $a_1 = 3$, $a_2 = 2$, $a_3 = 1$.

We are going prove that the assertion is true using strong induction on n. Assume that the assertion holds for any $n < k$, for some $k \geq 4$. We are going to show that the assertion also holds for k.

If $1 + 2 + \cdots + (k-1)$ is not a perfect square, then form the induction hypothesis we know that there is a suitable choice $a_1, a_2, \ldots, a_{k-1}$ from $\{1,2,\ldots,k-1\}$. Using these numbers, we set $a_k = k$ and note that a_1, a_2, …, a_{k-1}, $a_k = k$ is a k-tuple that satisfies the required condition.

If $1 + 2 + \vdots + (k-1) = \frac{(k-1)k}{2}$ is a perfect square, then the expression $1 + 2 + \cdots + (k-2) + k$ is not. By the induction hypothesis, we can choose distinct a_1, a_2, …, a_{k-2} from $\{1,2,\ldots,k-2\}$ satisfying the condition in the problem. Their sum

$$a_1 + a_2 + \cdots + a_{k-2} = 1 + 2 + \cdots + k - 2 = \frac{(k-2)(k-1)}{2}$$

is also not a square. To justify the last claim, suppose the contrary. Then, we can find $A, B \in \mathbb{N}^*$ such that $(k-2)(k-1) = 2A^2$ and $(k-1)k = 2B^2$. Multiplying the two equalities we can deduce that $(k-2)k$ must be a square. But this is a contradiction with the inequality $(k-2)^2 < (k-2)k < (k-1)^2$. In this case, we choose a_1, a_2, …, a_{k-2}, $a_{k-1} = k$, $a_k = k-1$ and note that the k-tuple satisfies the requested condition. The induction is now complete.

The following example appeared on shortlist of the International Mathematical Olympiad in 2006.

Example 3.28. *The sequence of real numbers $a_0, a_1, a_2, \ldots$ is defined recursively by*

$$a_0 = -1, \quad \sum_{k=0}^{n} \frac{a_{n-k}}{k+1} = 0, \quad \text{for} \quad n \geq 1.$$

Show that $a_n > 0$ for $n \geq 1$.

Solution. We prove the statement by induction on $n \geq 1$. For the base case, we note that $a_1 = 1/2$.

Now assume that $a_1, \ldots, a_{n-1} > 0$ for some $n \geq 2$. We note that a_n is positive if and only if $\sum_{k=1}^{n} \frac{a_{n-k}}{k+1}$ is negative. Now, since $a_1, \ldots, a_{n-1}$ are all positive, we know

$$\begin{aligned} -\frac{a_0}{n+1} = \frac{n}{n+1} \cdot \left(-\frac{a_0}{n}\right) &= \frac{n}{n+1} \sum_{k=0}^{n-2} \frac{a_{n-1-k}}{k+1} \\ &> \sum_{k=0}^{n-2} \frac{k+1}{k+2} \cdot \frac{a_{n-1-k}}{k+1} = \sum_{k=0}^{n-2} \frac{a_{n-1-k}}{k+2}. \end{aligned}$$

The inequality above implies that

$$\sum_{k=1}^{n} \frac{a_{n-k}}{k+1} = \frac{a_0}{n+1} + \sum_{k=1}^{n-1} \frac{a_{n-k}}{k+1} = \frac{a_0}{n+1} + \sum_{k=0}^{n-2} \frac{a_{n-1-k}}{k+2} < \frac{a_0}{n+1} - \frac{a_0}{n+1} = 0,$$

which completes the induction.

3.3.4 Mathematical induction - Cauchy form

Before seeing some examples using this technique, we introduce the principle of Cauchy induction, an elegant variation of mathematical induction.

Let P_n be a sequence of statements, and let n_0 be a positive integer. Suppose that the following hold:

1. P_{n_0} is true;
2. For $k \geq n_0$, P_k being true implies P_{2k} is true;
3. For $k \geq n_0$, P_{k+1} being true implies P_k is true.

Then we may conclude that P_n is true for all $n \geq n_0$.

As a first example, we give a proof of the AM–GM inequality, that is between the arithmetic and the geometric mean.

Example 3.29. *For any $n \in \mathbb{N}^*$ and any $a_1, a_2, \ldots, a_n \geq 0$, the following inequality holds*

$$\frac{a_1 + a_2 + \cdots + a_n}{n} \geq \sqrt[n]{a_1 a_2 \ldots a_n}.$$

Solution. Let P_n be the statement that for any $a_1, \ldots, a_n \geq 0$, we have

$$\frac{a_1 + a_2 + \cdots + a_n}{n} \geq \sqrt[n]{a_1 a_2 \ldots a_n}.$$

The statement P_1 is trivially true. Similarly, one can show that P_2 is equivalent to $(\sqrt{a_1} - \sqrt{a_2})^2 \geq 0$, hence true. Suppose that for some $k \in \mathbb{N}^*$, P_k is true. Consider $a_1, a_2, \ldots, a_k, a_{k+1}, \ldots, a_{2k} \geq 0$. Then

$$\frac{a_1 + a_2 + \cdots + a_{2k}}{2k} = \frac{\frac{a_1 + a_2 + \cdots + a_k}{k}}{2} + \frac{\frac{a_{k+1} + a_{k+2} + \cdots + a_{2k}}{k}}{2}.$$

Using the statement P_k for $a_1, a_2, \ldots, a_k$ and then for $a_{k+1}, a_{k+2}, \ldots, a_{2k}$ we get that the expression is greater or equal to

$$\sqrt[k]{a_1 a_2 \ldots a_k} + \sqrt[k]{a_{k+1} a_{k+2} \ldots a_{2k}} \geq \sqrt[2k]{a_1 a_2 \ldots a_{2k}},$$

where in the last inequality we used P_2. We just proved that for any $k \in \mathbb{N}^*$, P_k implies P_{2k}.

Now suppose P_{k+1} is true for some $k \in \mathbb{N}^*$. We want to show that this implies P_k is true. Let $a_1, a_2, \ldots a_k \geq 0$ be arbitrary.

Then by P_{k+1} true we have

$$\frac{a_1 + \cdots + a_k}{k} = \frac{a_1 + \cdots + a_k + \frac{a_1 + \cdots + a_k}{k}}{k+1} \geq \sqrt[k+1]{a_1 \cdots a_k \frac{a_1 + \cdots + a_k}{k}}.$$

Raising both terms to the power $k+1$, we get that

$$\left(\frac{a_1 + a_2 + \cdots + a_k}{k}\right)^{k+1} \geq a_1 a_2 \ldots a_k \frac{a_1 + a_2 + \cdots + a_k}{k}$$

which is equivalent to

$$\frac{a_1 + a_2 + \cdots + a_k}{k} \geq \sqrt[k]{a_1 a_2 \ldots a_k},$$

proving that P_{k+1} implies P_k.

The Cauchy induction is complete, hence P_n is true for all $n \in \mathbb{N}^*$.

Example 3.30 (Cauchy-Schwarz inequality). *Let $a_1, \ldots, a_n, b_1, \ldots, b_n$ be any real numbers. Then*

$$\left(a_1^2 + \ldots + a_n^2\right)\left(b_1^2 + \ldots + b_n^2\right) \geq (a_1 b_1 + \ldots + a_n b_n)^2.$$

Solution. We use Cauchy induction. For $n=1$ the inequality is clear. Also for $n=2$ we have to prove that $\left(a_1^2+a_2^2\right)\left(b_1^2+b_2^2\right)\geq\left(a_1b_1+a_2b_2\right)^2$, which after expanding the parentheses on both sides and simplification is equivalent to $a_1^2b_2^2+a_2^2b_1^2\geq 2a_1a_2b_1b_2\Leftrightarrow\left(a_1b_2-a_2b_1\right)^2\geq 0$.

Assume now that the inequality holds for some $n\geq 2$ and let us prove that it holds for $2n$. We need to show that

$$\left(a_1^2+\ldots+a_{2n}^2\right)\left(b_1^2+\ldots+b_{2n}^2\right)\geq\left(a_1b_1+\ldots+a_{2n}b_{2n}\right)^2$$

Let $x_1^2=a_1^2+\ldots+a_n^2$ (this substitution is possible as $a_1^2+\ldots+a_n^2\geq 0$),

$$x_2^2=a_{n+1}^2+\ldots+a_{2n}^2, y_1^2=b_1^2+\ldots+b_n^2, y_2^2=b_{n+1}^2+\ldots+b_{2n}^2$$

Then from the base case with two variables, we know that

$$\left(x_1^2+x_2^2\right)\left(y_1^2+y_2^2\right)\geq\left(x_1y_1+x_2y_2\right)^2$$

$P(n)$ implies further that

$$x_1y_1=\sqrt{\left(a_1^2+\ldots+a_n^2\right)\left(b_1^2+\ldots+b_n^2\right)}\geq\left(a_1b_1+\ldots+a_nb_n\right)$$

and similarly

$$x_2y_2\geq\left(a_{n+1}b_{n+1}+\ldots+a_{2n}b_{2n}\right)$$

Therefore

$$\left(x_1y_1+x_2y_2\right)^2\geq\left(a_1b_1+\ldots+a_{2n}b_{2n}\right)^2$$

which is what we wanted. Now we are left to prove that $P(n)\Rightarrow P(n-1)$. In other words, assuming that for any n variables we have

$$\left(a_1^2+\ldots+a_n^2\right)\left(b_1^2+\ldots+b_n^2\right)\geq\left(a_1b_1+\ldots+a_nb_n\right)^2$$

we want to prove that for any $n-1$ variables

$$\left(a_1^2+\ldots+a_{n-1}^2\right)\left(b_1^2+\ldots+b_{n-1}^2\right)\geq\left(a_1b_1+\ldots+a_{n-1}b_{n-1}\right)^2$$

This follows from $P(n)$ by simply setting $a_n=b_n=0$.

Example 3.31. *(USSR 1990) Assume that all coefficients of a quadratic polynomial $f(x)=ax^2+bx+c$ are positive and $a+b+c=1$. Prove that the inequality*

$$f\left(x_1\right)\cdots f\left(x_n\right)\geq 1$$

holds for all positive numbers $x_1,\ldots,x_n$, satisfying $x_1\cdots x_n=1$.

Solution. First observe that if $x_1 = 1$, we have $f(x_1) = a + b + c = 1$. We now prove that for any positive reals x and y we have $f(x) \cdot f(y) \geq (f(\sqrt{xy}))^2$.

Let $z = \sqrt{xy}$. Then one has

$$\begin{aligned} f(x) \cdot f(y) - (f(z))^2 &= a^2\left(x^2y^2 - z^4\right) + b^2\left(xy - z^2\right) + c^2(1-1) \\ &+ ab\left(x^2y + xy^2 - 2z^3\right) + ac\left(x^2 + y^2 - 2z^2\right) + bc(x + y - 2z) \\ &= ab\left(\sqrt{x^2y} - \sqrt{xy^2}\right)^2 + ac(x-y)^2 + bc(\sqrt{x} - \sqrt{y})^2 \geq 0 \end{aligned}$$

We now prove by induction that whenever n is a power of 2, for all positive reals $x_1, \ldots, x_n$ the following holds:

$$f(x_1) \cdots f(x_n) \geq \left(f\left(\sqrt[n]{x_1 \cdots x_n}\right)\right)^n$$

Assume that this is true for $n = 2^k$. Then using the inductive hypothesis and the inequality at the beginning, we obtain

$$\begin{aligned} f(x_1) \cdots f(x_{2^{k+1}}) &= \left(f(x_1) \cdots f(x_{2^k})\right) \cdot \left(f\left(x_{2^k+1}\right) \cdots f\left(x_{2^{k+1}}\right)\right) \\ &\geq \left(f\left(\sqrt[2^k]{x_1 \cdots x_{2^k}}\right) \cdot f\left(\sqrt[2^k]{x_{2^k+1} \cdots x_{2^{k+1}}}\right)\right)^{2^k} \\ &\geq \left(f\left(\sqrt[2^{k+1}]{x_1 \cdots x_{2^{k+1}}}\right)\right)^{2^{k+1}} \end{aligned}$$

and so the statement is also true for $n = 2^{k+1}$.

Suppose now that n is arbitrary and $x_1 \cdots x_n = 1$. Let k be the positive integer such that $2^{k-1} < n \leq 2^k$. Let us add, if necessary, $x_{n+1} = x_{n+2} = \ldots = x_{2^k} = 1$. Since $f(x_{n+1}) = f(x_{n+2}) = \ldots = f(x_{2^k}) = 1$, we may write

$$f(x_1) \cdots f(x_n) = f(x_1) \cdots f(x_{2^k}) \geq \left(f\left(\sqrt[2^k]{x_1 \cdots x_{2^k}}\right)\right)^{2^k} = 1,$$

and the induction is complete.

3.4 Erdös-Surányi sequences

The study of Erdős–Surányi sequences is motivated by their intriguing ability to represent integers through a simple combinatorial construction. To provide an intuitive understanding of these sequences, we start with a classical example illustrating their defining property using squares of integers.

Example 3.32 (Erdös-Surányi). *Show that for all $n \geq 1$, there is a k such that*

$$n = \pm 1^2 \pm 2^2 \pm \cdots \pm k^2,$$

for some choice of signs.

Solution. We use $n_0 = 1$ and $s = 4$ and verify the base cases P_1, P_2, P_3, P_4.

As $1 = +1^2$, $2 = -1^2 - 2^2 - 3^2 + 4^2$, $3 = -1^2 + 2^2$, $4 = -1^2 - 2^2 + 3^2$, this proves our base cases; we proceed to the inductive step, namely showing that P_k is true implies P_{k+4} is true. We claim that for all integers m, we have

$$m^2 - (m+1)^2 - (m+2)^2 + (m+3)^2 = 4.$$

We may note that

$$m^2 - (m^2 + 2m + 1) - (m^2 + 4m + 4) + (m^2 + 6m + 9) = 0m^2 + 0m + 4 = 4.$$

Now suppose that P_n holds; that is, we have

$$n = \pm 1^2 \pm 2^2 \pm \cdots \pm k^2$$

for some k. Then we may write

$$\begin{aligned}(\pm 1^2 \pm 2^2 \pm \cdots \pm k^2) + (k+1)^2 - (k+2)^2 - (k+3)^2 + (k+4)^2 = \\ n + (k+1)^2 - (k+2)^2 - (k+3)^2 + (k+4)^2 = n + 4.\end{aligned}$$

Hence $n + 4$ may be written in the desired form, so P_{n+4} is true. This completes our inductive step, hence P_n holds for all $n \geq 1$.

In fact, note that for each n there are infinitely many k for which there exists such a choice of signs. This is because, once you have such an expression for n, where the final term is k^2 one can repeatedly add

$$\begin{aligned}&\left[(k+1)^2 - (k+2)^2 - (k+3)^2 + (k+4)^2\right] \\ +&\left[-(k+5)^2 + (k+6)^2 + (k+7)^2 - (k+8)^2\right] = 4 + (-4) = 0,\end{aligned}$$

therefore obtaining infinitely many such representations of n.

In the example above, we show that $(a_n)_{n\geq 1}$, $a_n = n^2$, for all n belongs to a class of sequences that give rise to special representations of the integers. More precisely, a sequence of distinct positive integers $\{a_m\}_{m\geq 1}$ is called a **Erdös-Surányi sequence** if every integer may be written in the form

$$\pm a_1 \pm a_2 \pm \cdots \pm a_n$$

for some choices of signs $+$ and $-$, in infinitely many ways.

As an example of a Erdös-Surányi sequence we mention, for every $k \in \mathbb{N}$, $a_n = n^k$ (see J.Mitek, '79,[201]). For instance, for $k = 1$ we have

$$\begin{aligned}m = (-1 + 2) + (-3 + 4) + \cdots + (-(2m-1) + 2m) + \cdots + \\ + [(n+1) - (n+2) - (n+3) + (n+4)].\end{aligned}$$

For $k = 2$, the proof that the sequence $a_n = n^2$ is an Erdős–Surányi sequence is presented in the motivating example in this subsection.

For $k = 3$, one may use the identity

$$\begin{aligned}&-(m+1)^3+(m+2)^3+(m+3)^3-(m+4)^3\\&+(m+5)^3-(m+6)^3-(m+7)^3+(m+8)^3=48,\end{aligned}$$

and induction with a basis step for the first 48 positive integers. The fact that there are infinitely many such representations can be seen by adding 16 consecutive terms that cancel each other out, using the identity above.

Example 3.33. *Show that the sequence $(a_n)_{n\geq 1}$ given by $a_n = (2n-1)^2$ for all n is an Erdös-Surányi squence.*

Solution. The proof is based on induction with step 16 and the identity $16 = (2m+5)^2 - (2m+3)^2 - (2m+1)^2 + (2m-1)^2$. Given the identity, it therefore remains to check the first 16 cases, as follows

$$\begin{aligned}0&=-1^2+3^2+5^2-7^2+9^2-11^2-13^2+15^2\\1&=1^2\\2&=1^2+3^2+5^2-7^2+9^2-11^2-13^2+15^2\\3&=1^2-3^2+5^2+7^2+9^2+11^2+13^2-15^2-17^2-19^2+21^2\\4&=-1^2-3^2-5^2-7^2+9^2-11^2-13^2+15^2-17^2+19^2\\5&=1^2+3^2+5^2+7^2+9^2+11^2+13^2+15^2-17^2-19^2-21^2\\&\quad-23^2-25^2+27^2+29^2\\6&=-1^2-3^2+5^2-7^2-9^2+11^2\\7&=1^2+3^2+5^2+7^2+9^2+11^2+13^2+15^2+17^2-19^2+21^2\\&\quad-23^2-25^2-27^2+29^2\\8&=-1^2+3^2\\9&=-1^2-3^2+5^2-7^2-9^2-11^2-13^2-15^2-17^2+19^2-21^2\\&\quad-23^2-25^2-27^2+29^2+31^2+33^2\\10&=1^2+3^2\\11&=-1^2-3^2+5^2-7^2-9^2-11^2-13^2-15^2+17^2-19^2-21^2\\&\quad+23^2+25^2\\12&=-1^2-3^2-5^2-7^2+9^2+11^2-13^2+15^2+17^2\\13&=-1^2-3^2-5^2-7^2+9^2+11^2-13^2-15^2+17^2\\14&=-1^2-3^2-5^2+7^2\\15&=-1^2-3^2+5^2\end{aligned}$$

As before, adding a sequence of 8 consecutive terms that cancel each other out based on the identity

$$16 = (2m+5)^2 - (2m+3)^2 - (2m+1)^2 + (2m-1)^2,$$

one can see that for each n there are infinitely many such representations.

A sequence of distinct positive integers is **complete** if every positive integer can be written as a sum of some distinct terms of the sequence.

For instance, since every positive integer has a binary expansion, the sequence $a_n = 2^n$ for all $n \geq 0$ is complete.

We present an example which shows that the sequence of Fibonacci numbers, $F_0 = 0$, $F_1 = 1$ and $F_n = F_{n-1} + F_{n-2}$, for all $n \geq 2$ is complete.

Example 3.34 (Zeckendorf). *Show that if N is any positive integer, there exist positive integers $c_i \geq 2$, with $c_{i+1} > c_i + 1$, such that*

$$N = \sum_{i=0}^{k} F_{c_i}$$

where F_n is the n^{th} Fibonacci number.

Solution. This statement can be proved by strong induction induction. For $n = 1,2,3$ it is clearly true (as these are Fibonacci numbers), for $n = 4$ we have $4 = 3 + 1$. If n is a Fibonacci number then there is nothing to prove. Otherwise there exists j such that $F_j < n < F_{j+1}$. Now suppose each positive integer $a < n$ has such a representation (induction hypothesis) and consider $b = n - F_j$. Since $b < n$, b has such a representation by the induction hypothesis. At the same time, $b = n - F_j < F_{j+1} - F_j = F_{j-1}$, so the representation of b does not contain F_{j-1}, and hence also does not contain F_j. As a result, n can be represented as the sum of F_j and the representation of b, such that the Fibonacci numbers involved in the sum are distinct.

More generally, Zeckendorf's result also has a uniqueness part, which asserts that every positive integer can be represented uniquely as the sum of one or more distinct Fibonacci numbers in such a way that the sum does not include any two consecutive Fibonacci numbers. We give a brief proof.

First, one can easily prove by induction on n that sum of any non-empty set of distinct, non-consecutive Fibonacci numbers whose largest member is F_n is strictly less than F_{n+1}. We leave this an exercise for the reader.

Now take two non-empty sets A and B of distinct non-consecutive Fibonacci numbers which have the same sum, $\sum_{x \in S} x = \sum_{x \in T} x$. Consider sets A' and B' which are equal to A and B from which the common elements have been removed. Note that $\sum_{x \in A'} x = \sum_{x \in B'} x$.

We now prove that at least one of A' and B' is empty. Assume the contrary, i. e. that A' and B' are both non-empty and let the largest member of A' be F_s and the largest member of B' be F_t. Because A' and B' contain

no common elements, $F_s \neq F_t$. We can assume that $F_s < F_t$. Then by the result above, $\sum_{x\in A'} x < F_{s+1}$, and, by the fact that $F_s < F_{s+1} \leq F_t, \sum_{x\in A'} x < F_t$, whereas clearly $\sum_{x\in B'} x \geq F_t$. This contradicts the fact that A' and B' have the same sum, and we can conclude that either A' or A' must be empty.

If A' is empty. Then A' has sum 0, and so must B'. But since B' can only contain positive integers, it must be empty too. To conclude: $A' = B' = \emptyset$ which actually implies that the sets A and B were equal to begin with. This proves the uniqueness of the representation in Zeckendorf's result.

An important result concerning the Erdös-Surányi sequences is the following, which we present here with its proof, for brevity.

Theorem 3.1 (M.O. Drimbe, '83, [105]). *Let $\{a_m\}_{m\geq 1}$ be a sequence of distinct positive integers with $a_1 = 1$ and for every $n \geq 1$, $a_{n+1} \leq a_1 + \cdots + a_n + 1$. If $\{a_m\}_{m\geq 1}$ has infinitely many odd integers, then it is a Erdös-Surányi sequence.*

Proof. From the first hypothesis, it follows that the sequence $\{a_m\}_{m\geq 1}$ is complete. For details, we refer to the papers of J. L. Brown Jr. ([80], [81]) and that of M. O. Drimbe ([105]).

Following the recent papers of M. Tetiva ([248], [249]), let us denote by u_n the partial sum $a_1 + \cdots + a_n$, $n \geq 1$. Because the sequence $\{a_m\}_{m\geq 1}$ has infinitely many odd terms, it follows that u_p is even and odd for infinitely many p's. Let m be an arbitrary positive integer, and let p sufficiently large such that $u_p > m$, and u_p and m are of the same parity. The integer $s = (u_p - m)/2$ is less than u_p. Hence, it is the sum of some distinct terms of the sequence $\{a_m\}_{m\geq 1}$ with indices $\leq p$, that is

$$\frac{1}{2}\left(a_1 + \cdots + a_p - m\right) = \varepsilon_1 a_1 + \cdots + \varepsilon_p a_p,$$

for some $\varepsilon_1, \cdots, \varepsilon_p \in \{0,1\}$. The last relation is equivalent to

$$m = (1 - 2\varepsilon_1)a_1 + \cdots + (1 - 2\varepsilon_p)a_p,$$

with $1 - 2\varepsilon_1, \cdots, 1 - 2\varepsilon_p \in \{-1,1\}$, and the proof is finished since p can be selected in infinitely many ways. □

Unfortunately, the sequences mentioned above do not satisfy the condition $a_{n+1} \leq a_1 + \cdots + a_n + 1, n \geq 1$, in this theorem so, we cannot use this result to prove they are Erdös-Surányi sequences.

For an Erdös-Surányi sequence $\mathbf{a} = \{a_m\}_{m\geq 1}$, the **signum equation** of $\mathbf{a}$ is defined as

$$\pm a_1 \pm a_2 \pm \cdots \pm a_n = 0. \tag{3.1}$$

For a special case of the signum equation, see also the subsection 10.1.1.

Given a fixed integer n, a **solution** to the signum equation is a choice of signs $+$ and $-$ such that (3.1) holds. Denote by $S_{\mathbf{a}}(n)$ the number of solutions of the equation (3.1). Clearly, if 2 does not divide u_n, where $u_n = a_1 + \cdots + a_n$, then we have $S_{\mathbf{a}}(n) = 0$.

Here are few equivalent properties for $S_{\mathbf{a}}(n)$ (see [40]).

1. $S_{\mathbf{a}}(n)/2^n$ is the unique real number α having the property that the function $f:\mathbb{R}\to\mathbb{R}$, defined by

$$f(x)=\begin{cases}\cos\frac{a_1}{x}\cos\frac{a_2}{x}\cdots\cos\frac{a_n}{x} & \text{if } x\neq 0\\ \\ \alpha \text{ if } x=0,\end{cases}$$

   is a derivative.
2. $S_{\mathbf{a}}(n)$ is the term not depending on z in the development of

$$(z^{a_1}+\frac{1}{z^{a_1}})(z^{a_2}+\frac{1}{z^{a_2}})\cdots(z^{a_n}+\frac{1}{z^{a_n}}).$$

3. $S_{\mathbf{a}}(n)$ is the coefficient of $z^{u_n/2}$ in the polynomial

$$(1+z^{a_1})(1+z^{a_2})\cdots(1+z^{a_n}).$$

4. The following integral formula holds

$$S_{\mathbf{a}}(n)=\frac{2^{n-1}}{\pi}\int_0^{2\pi}\cos a_1t\cos a_2t\cdots\cos a_ntdt. \tag{3.2}$$

5. $S_{\mathbf{a}}(n)$ is the number of ordered bipartitions into classes having equal sums of the set $\{a_1,a_2,\cdots,a_n\}$.
6. $S_{\mathbf{a}}(n)$ is the number of partitions of $u_n/2$ into distinct parts, if 2 divides u_n, and $S_{\mathbf{a}}(n)=0$ otherwise.
7. $S_{\mathbf{a}}(n)$ is the number of distinct subsets of $\{a_1,a_2,\cdots,a_n\}$ whose elements sum to $u_n/2$ if 2 divides u_n, and $S_{\mathbf{a}}(n)=0$ otherwise.

To study the asymptotic behavior of $S_{\mathbf{a}}(n)$, when $n\to\infty$, is a very challenged problem. For instance, for the sequence $\mathbf{a}_k=(1^k,\ldots,n^k),k\geq 2$, it is still an open problem to show that

$$\lim_{n\to\infty}\frac{S_{\mathbf{a}_k}(n)}{2^n n^{-\frac{2k+1}{2}}}=\sqrt{\frac{2(2k+1)}{\pi}}.$$

For $k=1$ the previous relation was called the Andrica-Tomescu Conjecture [40] and it was proved by B.Sullivan [245].

For fixed positive integers n and k, one can also study the set $\mathcal{R}_k(n)$ of all integers that can be expressed as

$$\pm 1^k\pm 2^k\pm\cdots\pm n^k \tag{3.3}$$

for a choice of sign.

The following problem was proposed at the 2011 Romanian National Olympiad.

Example 3.35. *For every positive integer n, determine the set $\mathcal{R}_1(n)$.*

Solution. The greatest element of the set $\mathcal{R}_1(n)$ is the triangular number $T_n = 1 + 2 + \cdots + n = \frac{n(n+1)}{2}$, and the smallest element of $\mathcal{R}_1(n)$ is clearly $-T_n$. Also, the difference of any two elements of $\mathcal{R}_1(n)$ is an even number. Hence all elements of $\mathcal{R}_1(n)$ are of the same parity.

We claim that

$$\mathcal{R}_1(n) = \{-T_n, -T_n + 2, \ldots, T_n - 2, T_n\}. \tag{3.4}$$

Let us define a map on the elements of $\mathcal{R}_1(n) \setminus \{T_n\}$ having values in $\mathcal{R}_1(n)$. First, if $x \in \mathcal{R}_1(n) \setminus \{T_n\}$ is an element for which the writing begins with -1, then by changing -1 by $+1$, we get $x + 2 \in \mathcal{R}_1(n)$. If the writing of x begins with $+1$, then consider the first term in the sum which comes with a negative sign. Such a term exists unless $x = T_n$. In this case we have

$$x = 1 + 2 + \cdots + (j-1) - j \pm \cdots \pm n.$$

By changing the signs of terms $j - 1$ and j, it follows that $x + 2 \in \mathcal{R}_1(n)$. This shows the claim in (3.4).

One can wonder what happens if we work within classes modulo m with representations of the form (3.3). Of course, taking all the numbers in (3.4) modulo a small m, the chances are that all classes are covered. When m is a prime, there is an interesting and a more precise result related to this question which appeared as a problem in the Monthly ([193]).

Example 3.36. *Let p be an odd prime. Show that the $2^{(p-1)/2}$ numbers of the form $\pm 1 \pm 2 \pm \cdots \pm \frac{1}{2}(p-1)$ represent each nonzero residue class modulo p the same number of times. Determine this common number of representations and show that it differs by one from the number of representations of the zero residue class.*

Solution. Denote by $\zeta = e^{2\pi \mathrm{i}/p}$ and write

$$S = \left(\zeta + \zeta^{-1}\right)\left(\zeta^2 + \zeta^{-2}\right)\cdots\left(\zeta^{(p-1)/2} + \zeta^{-(p-1)/2}\right).$$

Then

$$S = a_0 + a_1\zeta + \cdots + a_{p-1}\zeta^{p-1}$$

where a_k is the number of ways k can be represented (mod p) by the expression $\pm 1 \pm 2 \pm \cdots \pm \frac{1}{2}(p-1)$.

Since S is also equal to

$$\left(\zeta^{(p+1)/2} + \zeta^{-(p+1)/2}\right)\cdots\left(\zeta^{p-1} + \zeta^{-(p-1)}\right)$$

we obtain

$$S^2 = \prod_{k=1}^{p-1}\left(\zeta^k + \zeta^{-k}\right) = \left(\prod_{k=1}^{p-1}\zeta^k\right)\left(\prod_{k=1}^{p-1}\left(1+\zeta^{-2k}\right)\right)$$
$$= \left(\zeta^{(p-1)p/2}\right)\left(\prod_{j=1}^{p-1}\left(1+\zeta^j\right)\right) = (1)\frac{(1)^p+(1)^p}{(1)+(1)} = 1,$$

where the identity $(x+y)(x+y\zeta)\left(x+y\zeta^2\right)\cdots\left(x+y\zeta^{p-1}\right) = x^p+y^p$ was used. This shows that $S \in \{-1,+1\}$. Since $1+x+x^2+\cdots+x^{p-1}$ is the minimal polynomial of ζ over the rationals, it follows that

$$a_0 - S = a_1 = a_2 = \cdots = a_{p-1}$$

Further, since $\zeta+\zeta^2+\cdots+\zeta^{p-1} = -1$ and

$$a_0 + (p-1)a_1 = a_0 + a_1 + \cdots + a_{p-1} = 2^{(p-1)/2},$$

we have

$$S = a_0 - a_1 = \left(2^{(p-1)/2} - (p-1)a_1\right) - a_1 = 2^{(p-1)/2} - pa_1$$
$$\equiv 2^{(p-1)/2} \bmod p,$$

so that $S = \left(\frac{2}{p}\right)$, where $\left(\frac{\cdot}{p}\right)$ is the Legendre symbol. Thus

$$a_1 = \frac{1}{p}\left(2^{(p-1)/2} - \left(\frac{2}{p}\right)\right) \quad \text{and} \quad a_0 = a_1 + \left(\frac{2}{p}\right).$$

For $k=2$ the situation with $\mathcal{R}_2(n)$ is almost the same as in case $k=1$ but there is an interesting new phenomenon, although expected since $\{m^2\}_{m\geq 1}$ is a Erdös-Surányi sequence as we have seen. Let us define the set

$$R_2(n) = \{-\textstyle\sum_2(n), -\sum_2(n)+2, \cdots, \sum_2(n)-2, \sum_2(n)\},$$

where $\sum_2(n) = 1^2+2^2+\cdots+n^2 = \frac{n(n+1)(2n+1)}{6}$.

Theorem 3.2. *For $n \in \mathbb{N}$, $\mathcal{R}_2(n) = R_2(n) \setminus \mathcal{E}_2(n)$, where*

$$\mathcal{E}_2(n) = \{\pm(\textstyle\sum_2(n) - 2j) : j \in E\} \text{ and}$$

$$E = \{2,3,6,7,8,11,12,15,18,19,22,23,24,27,28,31,32,33, \tag{3.5}$$
$$43,44,47,48,60,67,72,76,92,96,108,112,128\}.$$

Proof. The set E is known (see A001422 in OEIS) as being the set of all positive integers which cannot be written as a sum of distinct squares.

This is connected to a classical result of E. M. Wright ([261]) and to the papers of R. Sprague, P. T. Bateman, A. J. Hildebrand, and G. B. Purdy (see [241] and [61]). Let us observe that the equation

$$\pm 1^2 \pm 2^2 \pm 3^2 \cdots \pm n^2 = \sum\nolimits_2(n) - 2j$$

can be written equivalently as

$$2j = (1 \mp 1)1^2 + (1 \mp 1)2^2 + (1 \mp 1)3^2 + \cdots (1 \mp 1)n^2 \text{ or}$$

$$j = c_1 1^2 + c_2 2^2 + c_3 3^2 + \cdots + c_n n^2, \text{ with } c_i \in \{0,1\}.$$

So, a representation is possible if and only if j can be written as a sum of distinct perfect squares. It is known that the only positive integers that cannot be written as a sum of distinct squares are the ones in E. □

Chapter 4
Counting Strategies

Enumerative combinatorics is an area of combinatorics that deals with the number of ways that certain patterns can be formed. In enumerative combinatorics, a typical problem involves efficiently counting the size of a set of objects possessing certain properties.

4.1 Review on sets and functions

We will consider a set naively as a collection of objects called elements. We use the boldface letters $\mathbb{N}$ to denote the natural numbers (nonnegative integers) and $\mathbb{Z}$ to denote the integers. The boldface letters $\mathbb{R}$ and $\mathbb{C}$ shall respectively denote the real numbers and the complex numbers.

If S is a set and the element x is in the set, then we say that x belongs to S and we write this as $x \in S$. If x does not belong to S we write $x \notin S$. For example if $S = \{n \in \mathbb{N} \mid \text{n is the square of an integer}\}$, then $4 \in S$ but $2 \notin S$. We denote by $|A|$ the **cardinality** of A, that is, the number of elements that $|A|$ has. If a set A is totally contained in another set B, then we say that A is a subset of B and we write this as $A \subseteq B$ or $A \subset B$ if we are sure that $A \neq B$. For example, if $S = \{\text{squares of integers}\}$, then $A = \{1,4,9,16\}$ is a subset of S. If $x \in A$ and $x \notin B$ for some x, then A is not a subset of B, which we write as $A \not\subseteq B$. Two sets A and B are equal if $A \subseteq B$ and $B \subseteq A$.

Example 4.1. *Find all the subsets of* $\{a,b,c\}$.

Example 4.2. *Find all the subsets of* $\{a,b,c,d\}$.

Example 4.3. *Consider the set* $A = \{a \mid a \in \mathbb{N},\ 1 \leq n \leq 2009,\ 3|a\}$. *Find* $|A|$.

Solution. If $a \in A$ is an element of A, than a is of the form $a = 3k$ for some positive integer k. Since $a \leq 2009$, it follows that $3k \leq 2009$, that is $k \leq 669$. We can write $A = \{3k \mid k = 1,2,\ldots,669\}$, hence $|A| = 1003$.

Example 4.4. *Consider the set*

$$A = \{x \mid x \text{ is a positive integer and } 345 < 3x < 3210\}.$$

Find $|A|$.

Solution. From inequalities $345 < 3x < 3210$ we get $115 < x < 1070$, hence $116 \leq x \leq 1069$. The cardinal number of A is $|A| = 1069 - 115 = 954$.

The **union** of two sets A and B, is the set

$$A \cup B = \{x \mid x \in A \quad \text{or} \quad x \in B\}.$$

This is read A union B.

The **intersection** of two sets A and B, is

$$A \cap B = \{x \mid x \in A \quad \text{and} \quad x \in B\}.$$

This is read A intersection B.

The **difference** of two sets A and B, is

$$A \setminus B = \{x \mid x \in A \quad \text{and} \quad x \notin B\}.$$

The **symmetric difference** of two sets A and B, is the set

$$A \Delta B = (A \setminus B) \cup (B \setminus A).$$

The **complement** of A with respect to a set X such that $A \subseteq X$ is $\overline{A} = X \setminus A$. Observe that $\overline{A}$ is all that which is outside A. Usually we assume that A is a subset of some universal set U which is tacitly understood. The complement $\overline{A}$ represents the event that A does not occur.

Example 4.5. *Let* $U = \{0,1,2,3,4,5,6,7,8,9\}$ *be the universal set of the decimal digits and let* $A = \{0,2,4,6,8\} \subset U$ *be the set of even digits. Then* $\overline{A} = \{1,3,5,7,9\}$ *is the set of odd digits.*

Observe that

$$\overline{A} \cap A = \emptyset,$$

where $\emptyset$ is the empty set.

De Morgan Laws: If A and B share the same universal set, we have

$$\overline{A \cup B} = \overline{A} \cap \overline{B};$$
$$\overline{A \cap B} = \overline{A} \cup \overline{B}.$$

We will now prove one of the De Morgan Rules.

Example 4.6. *Prove the first De Morgan Law.*

Solution. Let $x \in \overline{A \cup B}$. Then $x \notin A \cup B$. Thus $x \notin A$ and $x \notin B$, that is, $x \in \overline{A}$ and $x \in \overline{B}$. This is the same as $x \in \overline{A} \cap \overline{B}$. Therefore we have the inclusion $\overline{A \cup B} \subseteq \overline{A} \cap \overline{B}$.

Now, let $x \in \overline{A} \cap \overline{B}$. Then $x \in \overline{A}$ and $x \in \overline{B}$. This means that $x \notin A$ and $x \notin B$ or what is the same $x \notin A \cup B$. But this last statement asserts that $x \in \overline{A \cup B}$. Hence $\overline{A} \cap \overline{B} \subseteq \overline{A \cup B}$. Since we have shown that the two sets contain each other, it must be the case that they are equal.

A **partition** of the set S is a collection of non-empty, pairwise disjoint subsets of S whose union is S.

Example 4.7. *Let* $2\mathbb{Z} = \{\cdots, -6, -4, -2, 0, 2, 4, 6, \cdots\}$ *be the set of even integers and let* $2\mathbb{Z}+1 = \{\ldots, -5, -3, -1, 1, 3, 5, \ldots\}$ *be the set of odd integers. Then* $2\mathbb{Z} \cup 2\mathbb{Z}+1 = \mathbb{Z}, (2\mathbb{Z}) \cap (2\mathbb{Z}+1) = \emptyset$*, and so* $\{2\mathbb{Z}, 2\mathbb{Z}+1\}$ *is a partition of* $\mathbb{Z}$*.*

Example 4.8. *The sets* $3\mathbb{Z}$, $3\mathbb{Z}+1$ *and* $3\mathbb{Z}+2$ *defined as*

- $3\mathbb{Z} = \{\cdots -9, -6, -3, 0, 3, 6, 9, \cdots\}$ *containing the integral multiples of* 3*;*
- $3\mathbb{Z}+1 = \{\ldots, -8, -5, -2, 1, 4, 7, \ldots\}$ *containing the integers leaving remainder* 1 *upon division by* 3*;*
- $3\mathbb{Z}+2 = \{\cdots, -7, -4, -1, 2, 5, 8, \ldots\}$ *containing the integers leaving remainder* 2 *upon division by* 3*,*

form a partition of $\mathbb{Z}$*, since* $(3\mathbb{Z}) \cup (3\mathbb{Z}+1) \cup (3\mathbb{Z}+2) = \mathbb{Z}$*, while*

$$(3\mathbb{Z}) \cap (3\mathbb{Z}+1) = \emptyset, (3\mathbb{Z}) \cap (3\mathbb{Z}+2) = \emptyset, (3\mathbb{Z}+1) \cap (3\mathbb{Z}+2) = \emptyset.$$

The **Cartesian product** of two sets A and B is the set

$$A \times B = \{(a,b) \mid a \in A \text{ and } b \in B\}.$$

The elements of $A \times B$ are called ordered pairs.

The **Cartesian product** of m sets $A_1, \ldots, A_m$ is defined as the set

$$A_1 \times \cdots \times A_m = \{(a_1, \ldots, a_m) \mid a_1 \in A_1, \ldots, a_m \in A_m\}.$$

The elements of $A_1 \times \cdots \times A_m$ are called ordered m-tuples.

Suppose A and B are sets. A **function** f from A to B (denoted as $f : A \to B$) is a relation associating to each $a \in A$ a unique element $b \in B$. The statement "associating" is abbreviated $f(a) = b$.

For a function $f : A \to B$, the set A is called the **domain** of f. (Think of the domain as the set of possible input values for f). The set B is called the **codomain** of f. The range of f is the set $\{f(a) \mid a \in A\}$. (Think of the **range** as the set of all possible output values for f. Think of the codomain as a sort of target for the outputs). The set $G_f = \{(a, f(a)) \mid a \in A\}$ is called the **graph** of function $f : A \to B$. Clearly, we have $G_f \subseteq A \times B$.

The **identity function** of the set A is $1_A : A \to A$, where for every $a \in A$ we have $1_A(a) = a$.

Two functions $f : A \to B$ and $g : C \to D$ are **equal** if $A = C, B = D$ and $f(a) = g(a)$ for every $a \in A$.

A function $f : A \to B$ is called:

1. **injective** (or one-to-one) if for every $x, y \in A, x \neq y$ implies $f(x) \neq f(y)$;
2. **surjective** (or onto) if for every $b \in B$ there is an $a \in A$ with $f(a) = b$;
3. **bijective** if f is both injective and surjective.

Let $f : A \to B$, $g : B \to C$ be two functions. The **composition** of g and f is a function $g \circ f : A \to C$, given by $(g \circ f)(a) = g(f(a)), (\forall)a \in A$. We have:

1. Associativity: $h \circ (g \circ f) = (h \circ g) \circ f$;
2. $f \circ 1_A = f$ and $1_B \circ f = f$;
3. If f and g are invertible, then $g \circ f$ is invertible and $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

$f : A \to B$ is injective $\Leftrightarrow$ there exists $g : B \to A$ such that $g \circ f = 1_A$.
$f : A \to B$ is surjective $\Leftrightarrow$ there exists $g : B \to A$ such that $f \circ g = 1_B$.

If a function $f : A \to B$ is bijective, then it has an inverse function denoted by $f^{-1} : B \to A$, satisfying the relations $f^{-1} \circ f = 1_A$ and $f \circ f^{-1} = 1_B$.

Example 4.9. *The function $f : \mathbb{R} \to \mathbb{R}$ defined as $f(x) = x^3 + 1$ is bijective. For finding its inverse we write $y = x^3 + 1$. Solving for x produces $x = \sqrt[3]{y-1}$, hence the inverse is the function $f^{-1} : \mathbb{R} \to \mathbb{R}$, where $f^{-1}(y) = \sqrt[3]{y-1}$.*

4.2 Simple counting principles

We begin by stating some simple counting principles that will allow us to solve a great wealth of combinatorics problems.

Addition Principle. *If event A can occur in a ways and event B can occur in b other ways, then the event of either A or B can occur in $a + b$ ways.*

The principle can be extended and applied for two or more events. The addition principle can be stated in terms of sets. Let S be a finite set, and let $S_1, S_2, \ldots, S_n$ be a partition of S. That is, $S_1 \cup S_2 \cup \ldots \cup S_n = S$, and $S_i \cap S_j = \emptyset$ when $i \neq j$. Then

$$|S| = |S_1| + |S_2| + \cdots + |S_n|,$$

where $|X|$ denotes the number of elements in the set X.

Multiplication Principle. *Let $A_1, A_2, \ldots, A_n$ be n independent events, and suppose that event A_i can occur in a_i different ways. The total number of ways that event A_1, followed by event A_2, ..., followed by event A_n can occur is $a_1 a_2 \cdots a_n$.*

We can also state the multiplication principle in terms of sets, that is, if we consider the finite sets $S_1, S_2, \ldots, S_n$ and

$$S = S_1 \times S_2 \times \cdots \times S_n = \{(s_1, s_2, \ldots, s_n) \mid s_i \in S_i,\ 1 \leq i \leq n\},$$

then $|S| = |S_1| \cdot |S_2| \cdot \ldots \cdot |S_n|$.

Example 4.10. *A code for a safe is a five-digit number that can have* 0 *in the first place as well in any other place. How many codes are there whose digits form an increasing sequence?*

Solution. We must consider only codes composed of different digits. Without the increasing order restriction we have $10 \cdot 9 \cdot 8 \cdot 7 \cdot 6 = 30240$ possibilities. But, only one of each of these possibilities has its digits in increasing order. It follows that, the desired number is

$$\frac{30240}{5 \cdot 4 \cdot 3 \cdot 2 \cdot 1} = \frac{30240}{120} = 252 = \binom{10}{5}.$$

Using the multiplication principle, we can prove the following, which is often convenient when dealing with combinations and permutations.

Division Principle. *If a list of length n contains every element of a set S exactly m times, then* $|S| = \frac{n}{m}$.

This principle is usually applied to problems in combinatorial set theory, combinatorial geometry, and number theory. It can be stated as follows.

Let S be a finite set, partitioned into k parts such that each part contains the same number of objects. Then the number of parts in the partition is

$$k = \frac{|S|}{\text{number of objects in a part}}.$$

While this may seem trivial, this principle has profound applications.

4.3 Permutations of sets

Numerous counting problems can be classified as one of the following types:

1. Count the ordered arrangements or ordered selections of objects
   a. without repeating any object
   b. with repetition of objects permitted (but perhaps limited).
2. Count the unordered arrangements or unordered selections of objects
   a. without repeating any object
   b. with repetition of objects permitted (but perhaps limited).

Instead of distinguishing between non-repetition and repetition of objects, we will distinguish between selections from a set and a multiset.

A **multiset** is like a set except that its members need not be distinct. For example, the sets $\{a,b\}$ and $\{a,a,b\}$ are the same, but the multisets $\{a,b\}$ and $\{a,a,b\}$ are not the same. Suppose a multiset M has three a's, one b, two c's and four d's. We will indicate the multiset by $\{3\cdot a,1\cdot b1,2\cdot c,4\cdot d\}$. The numbers 3;1;2;4 are called the repetition numbers of the multiset M. Clearly, a set is a multiset with all repetition numbers equal to 1. We can also allow infinite repetition numbers. Arrangements that take order into consideration are generally called **permutations** and **arrangements** where order is irrelevant are generally called combinations. So the four types of counting problems can be summarized as

1. permutations of sets
2. permutations of multisets
3. combinations of sets
4. combinations of multisets

Permutations of sets

Let r be a positive integer. By an **r-permutation** of a set S of n elements, we mean an ordered arrangement of r of the n elements.

For example, if S = $\{a,b,c\}$, we have three 1-permutations: a; b; c. We have six 2-permutations: *ab*; *ac*; *ba*; *bc*; *ca*; *cb* and six 3-permutations: *abc*; *acb*; *bac*; *bca*; *cab*; *cba*. There are no 4-permutations because the set has fewer than four elements.

The number of r-permutations of an n element set is denoted by $P(n;r)$. If $r > n$, then $P(n;r) = 0$, while $P(n;1) = n$ for every positive integer n. An n-permutation of an n element set will be called a **permutation** of the set.

Theorem 4.1. *For n and r positive integers with $r \leq n$ the following formula holds*

$$P(n;r) = n(n-1)\cdots(n-r+1).$$

Proof. There are n ways to choose the first item, $n-1$ ways to choose the second item, and so on until there are $n-(r-1) = n-r+1$ ways to choose the r^{th} item. Thus we have the result. □

For a nonnegative integer n, the **factorial** is defined by

$$n! = n(n-1)\cdots 2\cdot 1.$$

We use the convention that $0! = 1$. We can now write

$$P(n;r) = \frac{n!}{(n-r)!}.$$

For $n \geq 0$, define $P(n;0) = 1$ (the number of ways to choose no items from a set of n elements, i.e. the empty set), which agrees with the formula. The number of permutations of a set of size n is

$$P(n;n) = \frac{n!}{0!} = n!.$$

Theorem 4.2. *Let $A = \{a_1, \ldots, a_k\}$ and $B = \{b_1, \ldots, b_n\}$ be finite sets, $k \leq n$. Then*

1. *The number of injective functions $f : A \to B$ is $P(n;k)$.*
2. *The number of bijective functions $f : A \to A$ is $k!$.*

Proof. There are n ways to choose $f(a_1)$, $n-1$ ways to choose $f(a_2)$, and so on until there are $n-(k-1) = n-k+1$ ways to choose the $f(a_k)$. Thus we have $n(n-1)\cdots(n-k+1) = P(n;k)$ functions. □

For example, the number of words constructed with k distinct letters of an alphabet containing n letters is $P(n;k)$. Similarly, the number of ways to cover a rectangle of dimension $1 \times k$ by squares 1×1 of different colors from n colors is $P(n;k)$.

Circular permutations

The previous discussion thinks of objects as being in a line and are hence referred to as linear permutations. We can also arrange items in a circle (called, not surprisingly, **circular permutations**). The following serves as a good motivating example for this notion.

Suppose six children are marching in a circle. In how many different ways can they form their circle? Since the children are moving, what matters are their positions relative to each other and not to their environment. Thus, it is natural to regard two circular permutations as being the same provided one can be brought to the other by a rotation. There are six linear permutations for each circular permutation. For example, the circular permutation (126354) arises from each of the linear permutations

$$123456,\ 234561,\ 345612,\ 456123,\ 561234,\ 612345,$$

by regarding the last digit as coming before the first digit. Thus there is a 6-to-1 correspondence between the linear permutations of 6 children and the circular permutations of 6 children. Therefore, the number of circular permutations is $6!/6 = 5!$.

Theorem 4.3. *The number of circular r-permutations of n elements is given by*

$$\frac{P(n;r)}{r} = \frac{n!}{r(n-r)!}.$$

In particular, the number of circular permutations of n elements is $(n-1)!$.

Proof. The set of linear r-permutations can be partitioned into parts such that two linear r-permutations correspond to the same circular r-permutation if and only if they are in the same part. The number of circular r-permutations equals the number of parts. Since each part contains r linear r-permutations, we apply the division principle to arrive at the result. □

An alternate way of thinking about circular permutations: If we again consider the circular permutations of 6 children. Since we are free to rotate the children, think of the circle as a table and child 1 is at the "head" of the table. With that position fixed, the circular permutations of the six children can be identified with the linear permutations of children 2 through 5. There are 5! linear permutations of the thee remaining children and hence 5! circular permutations of six children.

4.4 Combinations of sets. Binomial expansion

Let S be a set of n elements. A **combination** of S is an unordered selection of the elements of S. The result of such a selection is a subset of S. Let r be a nonnegative integer. An unordered selection of r elements of S of n elements is called an r**-combination** of S, also called an r**-subset** of S. The number of r-subsets of an n element set is denoted $\binom{n}{r}$. Observe the following

$$\binom{n}{r} = \begin{cases} 0, & \text{if } r \geq n+1 \\ 0, & \text{if } n = 0 \text{ and } r \geq 1, \\ 1, & \text{if } r = 0, \\ n, & \text{if } r = 1, \\ 1, & \text{if } r = n. \end{cases}$$

Theorem 4.4. *For $0 \leq r \leq n$ the following formula holds*

$$P(n;r) = r!\binom{n}{r},$$

hence $\binom{n}{r} = \dfrac{n!}{r!(n-r)!}$.

Proof. Let S be an n element set. Each r-permutation of S is found by selecting r elements from S and ordering them. The number of ways to select r elements from S is $\binom{n}{r}$. The number of ways to order the r elements that have been selected is $r!$. By the multiplication principle, we have

$$P(n;r) = r!\binom{n}{r}.$$

Using the formula for $P(n;r)$, we get

$$\binom{n}{r} = \frac{P(n;r)}{r!} = \frac{n!}{r!(n-r)!},$$

and we are done. □

Corollary 4.1. *For $0 \leq r \leq n$, the following formula holds*

$$\binom{n}{r} = \binom{n}{n-r}.$$

Example 4.11. *Twenty five points are chosen in the plane so that no three of them are collinear. How many distinct straight lines do they form? How many distinct triangles do they form?*

Solution. Given 25 points in the plane, no tree of them collinear, the number of distinct straight lines that can be formed by joining any two of them is given by the number of subsets of cardinality 2 chosen from a subset of cardinality 25, namely $\binom{25}{2} = \frac{25 \cdot 24}{2} = 300$.

Each 3 distinct points determine a triangle, so to count the number of distinct triangles that can be formed by these 25 points, we can use the formula

$$\binom{25}{3} = \frac{25!}{3!(25-3)!} = \frac{25 \cdot 24 \cdot 23}{3 \cdot 2 \cdot 1} = 2300.$$

Hence, we have 300 distinct straight lines and 2300 distinct triangles that can be formed from 25 planar points, if no three of them are collinear.

Example 4.12. *How many eight letter "words" can be constructed by using the* 26 *letters of the alphabet if each word contains* 3, 4, *or* 5 *vowels? It is understood that there is no restriction on the number of times a letter can be used in a word.*

Solution. We can solve this problem by breaking it down into cases based on the number of vowels in the word.

Case 1: The word contains 3 vowels. In this case, there are $\binom{8}{3}$ ways to choose the positions of the vowels in the word, and for each vowel position, there are 5 choices for the vowel and 21 choices for the consonant. Therefore, the total number of 8-letter words with 3 vowels is $\binom{8}{3} \cdot 5^3 \cdot 21^5$.

Case 2: Similarly, when the word contains 4 vowels, we get $\binom{8}{4} \cdot 5^4 \cdot 21^4$.

Case 3: When the word contains 5 vowels, we get $\binom{8}{5} \cdot 5^5 \cdot 21^3$.

Therefore, the total number of 8-letter words with 3, 4, or 5 vowels is the sum of the results from each case:

$$\binom{8}{3} \cdot 5^3 \cdot 21^5 + \binom{8}{4} \cdot 5^4 \cdot 21^4 + \binom{8}{5} \cdot 5^5 \cdot 21^3.$$

Theorem 4.5 (Pascal's Formula). *For all integers n,k with $1 \leq k \leq n-1$, we get*

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

Proof. One could prove this theorem using the formula in Theorem 1. However, we will give a combinatorial proof. Let S be a set of n elements. Choose one specific element of S called x. Let $S \setminus \{x\}$ be the set obtained from S by removing x. Partition the set X of k-subsets of S into two parts, A and B. Part A will contain all k-subsets of S that do not contain x. Part B will contain all k-subsets of S that contain x. The size of X is $\binom{n}{k}$ by definition. By the addition principle, we also have $|X| = |A| + |B|$. The k-subsets in A are exactly the k-subsets of the set $S \setminus \{x\}$ of $n-1$ elements, so the size of A is

$$|A| = \binom{n-1}{k}.$$

A k-subset in B can be found by finding a $k-1$- subset of the set $S \setminus \{x\}$ of $n-1$ elements and appending an x, so the size of B is

$$|B| = \binom{n-1}{k-1}.$$

Combining the facts, we have

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

□

Theorem 4.6. *For $n \geq 0$*

$$\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{n} = 2^n.$$

Proof. Let S be an n element set. Every subset of S is an r-subset of S for $r = 0,1,\ldots,n$. Since $\binom{n}{1}$ is the number of r-subsets of S, it follows that

$$\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{n} = 2^n$$

is the number of subsets of S.

We can also count the number of subsets of S by considering each element of S in turn. For each element we have 2 options: either the element is in a subset or it is not. So there are 2^n subsets of S. The two formulas count the same thing, so they must be equal and we have our result. □

The numbers $\binom{n}{k}$ count the number of k-subsets of a set of n elements. They are called **binomial coefficients** and feature in the binomial theorem. These numbers satisfy a number of identities and have interesting properties that are useful in the analysis of algorithms.

The following properties hold:

1. For $k \leq \left\lceil \frac{n}{2} \right\rceil$, $\binom{n}{k}$ is a polynomial in variable n of degree k.
2. (Symmetry) $\binom{n}{k} = \binom{n}{n-k}$.
3. (Pascal's formula) $\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}, \quad 1 \leq k \leq n-1.$
4. (Recursive formulas)
   a. $\binom{n}{k} = \frac{n}{k}\binom{n-1}{k-1}, \quad 1 \leq k \leq n-1.$
   b. $\binom{n}{k} = \frac{k+1}{n+1}\binom{n+1}{k+1}, \quad 0 \leq k \leq n.$

By Pascal's formula and $\binom{n}{0} = 1$ and $\binom{n}{n} = 1$, we can derive the binomial coefficients without using the third formula above. The results are often displayed in an infinite array called Pascal's triangle.

Theorem 4.7 (Binomial expansion). *Let n be a positive integer. Then for all x and y, the following formula holds:*

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k,$$

a homogeneous symmetric polynomial in x and y of degree n with $n+1$ terms.

Proof 1. (By counting the terms) Write $(x+y)^n$ as the product

$$(x+y)(x+y)\cdots(x+y)$$

of n factors of $x+y$. Fully expand this product using the distributive law and group terms alike. For each factor $x+y$ we can choose either x or y in $(x+y)^n$, so there are 2^n terms. Each can be arranged in the form $x^{n-k}y^k$ for some $k = 0, 1, \ldots, n$. We obtain term $x^{n-k}y^k$ by choosing y in k of the n factors and x in the remaining $n-k$ factors. Thus, the term $x^{n-k}y^k$ occurs $\binom{n}{k}$ times in the expanded product. Hence we have our result. □

Proof 2. (By induction) Our base case $n = 1$ cleary holds:

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

Assuming that the theorem holds for n, we show it holds for $n+1$. Write

$$(x+y)^{n+1} = (x+y)(x+y)^n,$$

which, by the induction hypothesis (the binomial theorem for n), becomes

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

Replace the index k by $k-1$ and adjust the limits in the second summation in the last line to obtain

$$\sum_{k=0}^{n-1}\binom{n}{k}x^{n-k}y^{k+1} = \sum_{k=1}^{n}\binom{n}{k-1}x^{n+1-k}y^k.$$

Thus we have

$$(x+y)^{n+1} = x^{n+1} + \sum_{k=1}^{n}\left[\binom{n}{k} + \binom{n}{k-1}\right]x^{n+1-k}y^k + y^{n+1},$$

which by Pascal's formula can be rewritten as

$$(x+y)^{n+1} = x^{n+1} + \sum_{k=1}^{n}\binom{n+1}{k}x^{n+1-k}y^k + y^{n+1} = \sum_{k=0}^{n+1}\binom{n+1}{k}x^{n+1-k}y^k,$$

and we have our result. □

The **generic term** in this expansion is $T_{k+1} = \binom{n}{k}a^{n-k}b^k$ and it is situated in position $k+1$. The recursive formula for the generic term is

$$T_{k+2} = \frac{n-k}{k+1}\cdot\frac{b}{a}T_{k+1}.$$

For $x = y = 1$ in the binomial expansion we get

$$\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{n-1} + \binom{n}{n} = 2^n.$$

For $x = 1, y = -1$ in the binomial expansion we get

$$\binom{n}{0} - \binom{n}{1} + \cdots + (-1)^n \binom{n}{n} = 0, \quad n \geq 1,$$

hence we have

$$\binom{n}{0} + \binom{n}{2} + \cdots = \binom{n}{1} + \binom{n}{3} + \cdots = 2^{n-1}.$$

4.5 Extended binomial expansion

Now we extend the definition of $\binom{n}{k}$ to allow n to be any real number and k any integer. Let α be a real number and let k be an integer. Define the **extended binomial coefficient** as

$$\binom{\alpha}{k} = \begin{cases} \frac{\alpha(\alpha-1)\cdots(\alpha-k+1)}{k!} & \text{if } k \geq 1 \\ 1 & \text{if } k = 0 \\ 0 & \text{if } k \leq -1 \end{cases} . \tag{4.1}$$

Remark. In the case $k \geq 1$, $\binom{\alpha}{k}$ is a polynomial in α of degree k with the leading coefficient $\frac{1}{k!}$.

Example 4.13. *Compute* $\binom{1/2}{2}$.

Solution. Using the definition we have

$$\binom{1/2}{2} = \frac{1/2(1/2-1)}{2!} = -\frac{1}{8}.$$

Theorem 4.8 (Extended Pascal's Formula). *For all real numbers α and all integers k, we have*

$$\binom{\alpha}{k} = \binom{\alpha-1}{k} + \binom{\alpha-1}{k-1}.$$

Proof. If $k \leq -1$ the relation is clear. If $k = 0$ this reduces to $\alpha = (\alpha - 1) + 1$, also clear. If $k \geq 1$, after simplification, the relation is equivalent to

$$\frac{\alpha}{k} = \frac{\alpha - k}{k} + 1.$$

which is obvious. □

Isaac Newton generalized the binomial theorem to obtain an expansion for $(x+y)^\alpha$ where α is any real number. In general, the expansion becomes an infinite series and questions of convergence need to be considered. We will restrict ourselves to a statement of the theorem and some special cases.

Theorem 4.9 (Extended binomial expansion). *Let α be a real number. Then for all x and y, with $0 \leq |x| < |y|$, the following formula holds:*

$$(x+y)^\alpha = \sum_{k=0}^{\infty} \binom{\alpha}{k} x^k y^{\alpha-k}.$$

Proof. The formula is equivalent to

$$\left(1+\frac{x}{y}\right)^\alpha = \sum_{k=0}^{\infty} \binom{\alpha}{k} \left(\frac{x}{y}\right)^k,$$

that is

$$(1+t)^\alpha = \sum_{k=0}^{\infty} \binom{\alpha}{k} t^k,$$

where $t = \frac{x}{y} < 1$. Consider the function $f : (-1,1) \to \mathbb{R}$, defined by the formula $f(t) = (1+t)^\alpha$. By Taylor's expansion formula, we have

$$f(t) = f(0) + \frac{f'(0)}{1!}t + \frac{f''(0)}{2!}t^2 + \cdots = \sum_{k=0}^{\infty} \frac{f^{(k)}(0)}{k!} t^k.$$

In our case we have

$$f^{(k)}(t) = \alpha(\alpha-1)\cdots(\alpha-k+1)(t+1)^{\alpha-k},$$

hence

$$f^{(k)}(0) = \alpha(\alpha-1)\cdots(\alpha-k+1),$$

and the formula is proved. □

In practice, the following particular form of the formula is often used:

Corollary 4.2.

$$(1+t)^\alpha = \sum_{k=0}^{\infty} \binom{\alpha}{k} t^k.$$

The generic term of the expansion is

$$T_{k+1} = \binom{\alpha}{k} t^k,$$

and it is situated at the position $k+1$.

Example 4.14. *If $|t| < 1$ and n a positive integer, prove the relation*

$$\frac{1}{(1-t)^n} = \sum_{k=0}^{\infty} \binom{n+k-1}{k} t^k.$$

Solution. Take $\alpha = -n$ and obtain

$$\begin{aligned}\binom{\alpha}{k} = \binom{-n}{k} &= \frac{(-n)(-n-1)\cdots(-n-k+1)}{k!} \\ &= (-1)^k \frac{n(n+1)\cdots(n+k-1)}{k!} = (-1)^k \binom{n+k-1}{k}.\end{aligned}$$

Now, from the extended binomial expansion we get

$$(1+t)^{-n} = \sum_{k=0}^{\infty} \binom{-n}{k} = \sum_{k=0}^{\infty} (-1)^k \binom{n+k-1}{k} t^k.$$

Replace t by $-t$ and obtain

$$\begin{aligned}(1-t)^{-n} &= \sum_{k=0}^{\infty} (-1)^k \binom{n+k-1}{k} (-t)^k \\ &= \sum_{k=0}^{\infty} (-1)^k (-1)^k \binom{n+k-1}{k} t^k,\end{aligned}$$

and we are done.

4.6 Permutations of multisets

Recall that a **multiset** is like a set except that its members need not be distinct. For example, the sets $\{a;b\}$ and $\{a;a;b\}$ are the same, but the multisets $\{a;b\}$ and $\{a;a;b\}$ are not the same. Suppose a multiset M has three a's, one b, two c's and four d's. We will indicate the multiset by $\{3.a;1.b;2.c;4.d\}$. The numbers 3;1;2;4 are called the **repetition numbers** of the multiset M. A set is a multiset with all repetition numbers equal to 1. We can also allow infinite repetition numbers. In this case we will use ∞ to indicate that the repetition number is infinite.

If S is a multiset, an r-**permutation** of S is an ordered arrangement of r of the objects of S. If the total number of objects in S is n (counting repetitions), then an n-permutation of S will simply be called a **permutation** of S.

We note that for $S = \{3.a;2.b;1.c\}$, then *abcab*, *baaab* are 5-permutations of S and *abcaba* is a permutation of S. The multiset S has no 7-permutations since $7 > 3+2+1 = 6$, the number of objects of S.

Theorem 4.10. *Let S be a multiset with objects of k different types, where each object has an infinite repetition number. The number of r-permutations of S is k^r.*

Proof. In constructing any r-permutation of S, we can choose the first item to be an object of any one of the k types. Similarly, the second item can be an object of any one of the k types. Since the repetition numbers are infinite, there are k ways to choose each item. By the multiplication principle there are k^r ways to choose the r items. □

Note that the conclusion of the theorem remains true if the repetition numbers of the k different types of objects of S are all at least r (that is we can't run out of items of any type).

Theorem 4.11. *Let S be a multiset with objects of k different types with finite repetition numbers $n_1; n_2; \cdots; n_k$, respectively. If the size of S is $n = n_1 + n_2 + \cdots + n_k$, then the number of permutations of S is*

$$\frac{n!}{n_1!n_2!\cdots n_k!}.$$

Proof 1. Suppose S has objects of k types, say $a_1, a_2, \ldots, a_k$, with repetition numbers $n_1; n_2; \cdots; n_k$ for a total of $n = n_1 + n_2 + \cdots + n_k$ objects. To determine the number of n-permutations, we have to put exactly one of the objects of S in each of n places. First decide which places will by occupied by a_1's. There are n_1 objects of type a_1 in S, so there are $\binom{n}{n_1}$ ways to place the a_1's. Next decide where to put the a_2's. There are n_2 objects of type a_2 in S and $n - n_1$ places remaining, so there are $\binom{n-n_1}{n_2}$ ways to place the a_2's. Continuing this, we see the number of n-permutations of S is

$$\binom{n}{n_1}\binom{n-n_1}{n_2}\binom{n-n_1-n_2}{n_3}\cdots\binom{n-n_1-n_2-\cdots-n_{k-1}}{n_k}$$

which can be expressed as

$$\frac{n!}{n_1!(n-n_1)!}\cdot\frac{(n-n_1)!}{n_2!(n-n_1-n_2)!}\cdots\frac{(n-n_1-n_2-\cdots-n_{k-1})!}{n_k!(n-n_1-n_2-\cdots-n_k)!}.$$

This simplifies to $\dfrac{n!}{n_1!n_2!\cdots n_k!0!} = \dfrac{n!}{n_1!n_2!\cdots n_k!}$. □

Proof 2. If S has n elements, then the number of permutations of S is $n!$. But for a fixed permutations, we have $n_1!$ permutations of a_1's that give the same permutation of the multiset S. Also, we have $n_2!$ permutations of a_2's giving the same permutation of the multiset S, and so on, $n_k!$ permutations of a_k's that give the same permutation of the multiset S. By the division principle, the number of all permutation of the multiset S is $\dfrac{n!}{n_1!n_2!\cdots n_k!}$. □

Remark. From Theorem (4.11), it follows that the number

$$\frac{n!}{n_1!n_2!\cdots n_k!}$$

is an integer, that is $n_1!n_2!\cdots n_k!$ divides $(n_1+n_2+\cdots+n_k)!$.

Example 4.15. *Find the number of permutations of the letters of the word*

$$ADDRESSES.$$

Solution. The multiset is $\{1.A;2.D;2.E;1.R;3.S\}$. The repetition numbers are $n_1=1;n_2=2;n_3=2;n_4=1;n_5=3$, and the total number of objects is given by $n=n_1+\cdots+n_5=1+2+2+1+3=9$. By the formula in Theorem 4.11, the number of permutations is

$$\frac{n!}{n_1!n_2!n_3!n_4!n_5!}=\frac{9!}{1!2!2!1!3!}=15120.$$

Theorem 4.12. *Let n be a positive integer and let $n_1;n_2;\cdots;n_k$ be positive integers with $n=n_1+n_2+\cdots+n_k$. The number of ways to partition a set of n objects into k labeled boxes in which Box 1 contains n_1 objects, Box 2 contains n_2 objects and so on is*

$$\frac{n!}{n_1!n_2!\cdots n_k!}.$$

If boxes are not labeled and $n_1=n_2=\cdots=n_k$, then the number of partitions is

$$\frac{n!}{k!n_1!n_2!\cdots n_k!}.$$

Proof. First choose n_1 objects for the first box. This can be done $\binom{n}{n_1}$ ways. Next, choose n_2 of the remaining $n-n_1$ objects for the second box. This can be done in $\binom{n-n_1}{n_2}$ ways. Continue in this way and by the multiplication principle, the number of ways to partition the items is

$$\binom{n}{n_1}\binom{n-n_1}{n_2}\binom{n-n_1-n_2}{n_3}\cdots\binom{n-n_1-n_2-\cdots-n_{k-1}}{n_k},$$

which we saw in the proof of Theorem 4.11

$$\frac{n!}{n_1!n_2!\cdots n_k!}.$$

If the boxes are not labeled and $n_1=n_2=\cdots=n_k$, for each of way of allocating the objects into the k unlabeled boxes, there are $k!$ ways to attach the labels. Thus by the division principle, the number of ways to partition n objects equally into k unlabeled boxes is $\frac{n!}{k!n_1!n_2!\cdots n_k!}$. □

4.7 Combinations of multisets

If S is a multiset, an r-**combination** of S is an unordered arrangement of r of the objects of S. If the total number of objects in S is n (counting repetitions), then an n-combination of S will simply be S.

Example 4.16. *If* $S = \{3.a; 2.b; 1.c\}$, *then the* 3*-combinations of* S *are*

$$\{3.a\}; \{2.a; 1.b\}; \{2.a; 1.c\}; \{1.a; 2.b\}; \{1.a; 1.b; 1.c\}; \{2.b; 1.c\}.$$

There are no 7*-combinations as* $7 > 3 + 2 + 1 = 6$, *the number of objects of* S.

Theorem 4.13 (De Moivre). *Let* r *be a positive integer. The equation*

$$x_1 + x_2 + \cdots + x_k = r$$

has $\binom{r-1}{k-1}$ *positive integer solutions.*

Proof. We write r as $r = 1 + 1 + \cdots + 1 + 1$, where there are r copies of 1s and $r - 1$ signs $+$. To decompose r in k summands we only need to choose $k - 1$ pluses from the $r - 1$, which proves the theorem. □

Corollary 4.3. *Let* r *be a positive integer. The equation*

$$y_1 + y_2 + \cdots + y_k = r$$

has $\displaystyle\binom{n + r - 1}{r - 1}$ *non-negative integer solutions.*

Proof. Denoting $x_j - 1 = y_j$, $j = 1, 2, \ldots, k$, one has $x_j \geq 1$. Then the equation $x_1 - 1 + x_2 - 1 + \cdots + x_k - 1 = r$ is equivalent to $x_1 + x_2 + \cdots + x_k = r + k$, which from Theorem 1, has $\binom{r+k-1}{k-1}$ solutions. □

Theorem 4.14. *Let* S *be a multiset with objects of* k *different types, where each object has an infinite repetition number. Then the number of* r*-combinations of* S *is*

$$\binom{r + k - 1}{r} = \binom{r + k - 1}{k - 1}.$$

Proof. Let the k types of objects of S be $a_1, a_2, \ldots, a_k$ so that

$$S = \{\infty.a_1; \infty.a_2; \cdots; \infty.a_k\}.$$

Any r-combination of S is of the form

$$\{x_1.a_1; x_2.a_2; \cdots; x_k.a_k\},$$

where $x_1, x_2, \ldots, x_k$ are nonnegative integers with $x_1 + x_2 + \cdots + x_k = r$.

Conversely, every sequence $x_1, x_2, \ldots, x_k$ of nonnegative integers with $x_1 + x_2 + \cdots + x_k = r$ corresponds to an r-combination of S.

Thus there is a one-to-one correspondence between the number of r-combinations of S and the number of solutions of the equation

$$x_1 + x_2 + \cdots + x_k = r, \tag{4.2}$$

where $x_1, x_2, \ldots, x_k$ are nonnegative integers. So the number of r-combinations of S is equal to the number of solutions to the equation (2), where $x_1, x_2, \ldots, x_k$ are nonnegative integers. According to the previous Corollary this number is equal to $\binom{r+k-1}{r} = \binom{r+k-1}{k-1}$. □

Remark. 1°. We can give a direct combinatorial argument for the formula in the Corollary, that is to count the number of solutions to equation (2). In this respect, let us consider the multiset

$$M = \{r.1; (k-1).0\}.$$

The $k-1$ 0's divided the r 1's into k groups as follows. Let there be x_1 1's to the left of the first 0, x_2 1's between the first and second 0, and so on, with x_k 1's to the right of the last 0. Then $x_1, x_2, \ldots, x_k$ are nonnegative integers with $x_1 + x_2 + \cdots + x_k = r$. Conversely, given nonnegative integers $x_1, x_2, \ldots, x_k$ with $x_1 + x_2 + \cdots + x_k = r$, we can construct a permutation of the multiset M. Thus there is a one-to-one correspondence between the number of r-permutations of the multiset M and the number of solutions to the equation (4.2) with $x_1, x_2, \ldots, x_k$ nonnegative, that is we have a one-to-one correspondence between the number of r-permutations of M and the number of r-combinations of S. So the number of r-combinations of S is equal to the number of r-permutations of M which, by Theorem 4.1 is

$$\frac{(r+k-1)!}{r!(k-1)!} = \binom{r+k-1}{r}.$$

2°. Note that the conclusion of the theorem remains true if the repetition numbers of the k different types of objects of S are all at least r (i.e. we can't run out of items of any type).

3°. There is no general formula for finding the number of r-combinations of an n element multiset $S = \{n_1.a_1; n_2.a_2; \cdots; n_k.a_k\}$, $r < n$. The number of r-combinations of S is equal to the number of integral solutions of $x_1 + x_2 + \cdots + x_k = r$, where $0 \le x_1 \le n_1, 0 \le x_2 \le n_2, \ldots, 0 \le x_k \le n_k$. The upper bounds cannot be handled the same way we treated the lower bounds.

4.8 Multinomial expansion

We can generalize the binomial theorem to find a formula for the n-th power of the sum of k real numbers:

$$(x_1 + x_2 + \cdots + x_k)^n.$$

In general, the role of the binomial coefficients is taken over by numbers called **multinomial coefficients**, defined as

$$\binom{n}{n_1, n_2, \ldots, n_k} = \frac{n!}{n_1! n_2! \cdots n_k!},$$

where $n_1, n_2, \ldots, n_k$ are nonnegative integers with $n_1 + n_2 + \cdots + n_k = n$.

Recall that this number represents the number of permutations of a multiset of n objects of k different types with repetition numbers $n_1, n_2, \ldots, n_k$, respectively. The binomial coefficients are just multinomial coefficients with $k = 2$, which gives

$$\binom{n}{j} = \binom{n}{j, n-j},$$

and represent the number of permutations of a multiset of n objects of 2 types with repetition numbers j and $n - j$, respectively.

Theorem 4.15 (Pascal's formula for multinomials). *For the positive integers n, n_1, $n_2, \ldots, n_k$ with $n_1 + n_2 + \cdots + n_k = n$, the following formula holds:*

$$\binom{n}{n_1, n_2, \ldots, n_k} = \binom{n-1}{n_1 - 1, n_2, \ldots, n_k} + \cdots + \binom{n-1}{n_1, n_2, \ldots, n_k - 1}.$$

Proof. Just replace the formula of the multinomial coefficients and, after simplification we get the equivalent form

$$\frac{n}{n_1 n_2 \cdots n_k} = \frac{1}{n_2 \cdots n_k} + \cdots + \frac{1}{n_1 \cdots n_{k-1}},$$

which is clearly true. □

Theorem 4.16 (Multinomial expansion). *Let n be a positive integer. For all $x_1, x_2, \ldots, x_k$ the following formula holds:*

$$(x_1 + x_2 + \cdots + x_k)^n = \sum \binom{n}{n_1, n_2, \ldots, n_k} x_1^{n_1} x_2^{n_2} \cdots x_k^{n_k},$$

where the summation extends over all nonnegative integral solutions $n_1, n_2, \ldots, n_k$ of the equation $n_1 + n_2 + \cdots + n_k = n$.

Proof. Write $(x_1 + x_2 + \cdots + x_k)^n$ as a product of n factors, each equal to $(x_1 + x_2 + \cdots + x_k)$. Completely expand the product, using the distributive law and collect like terms. For each of the n factors, we choose one of the k numbers $x_1, x_2, \ldots, x_k$ and form their product. There are k^n terms that result this way, and each can be arranged in the form $x^{n_1}x^{n_2}\cdots x^{n_k}$, where $n_1, n_2, \ldots, n_k$ are nonnegative integers summing to n. We obtain the term $x_1^{n_1}x_2^{n_2}\cdots x_k^{n_k}$ by choosing x_1 in n_1 of the n factors, x_2 in n_2 of the remaining $n - n_1$ factors, on down to x_k in n_k of the remaining $n - n_1 - \cdots - n_{k-1}$. By the multiplication principle, the number of times the term $x_1^{n_1}x_2^{n_2}\cdots x_k^{n_k}$ is given by

$$\binom{n}{n_1}\binom{n-n_1}{n_2}\binom{n-n_1-n_2}{n_3}\cdots\binom{n-n_1-n_2-\cdots-n_{k-1}}{n_k},$$

which we know from the proof of Theorem 4.11, is equal to

$$\frac{n!}{n_1!n_2!\cdots n_k!} = \binom{n}{n_1, n_2, \ldots, n_k}.$$

□

Remark. The number of terms in the multinomial expansion is the number of solutions in nonnegative integers of the equation $n_1 + n_2 + \cdots + n_k = n$. According to Corollary 4.3, this is given by

$$\binom{n+k-1}{n}.$$

In case $k = 2$, by the previous formula we obtain

$$\binom{n+2-1}{n} = \binom{n+1}{n} = n + 1,$$

i.e. the number of terms in the classical binomial expansion $(x_1 + x_2)^n$.

For example, consider the multinomial with $k = 3$ and $n = 3$, that is

$$(x_1 + x_2 + x_3)^3.$$

After expansion we will find $\binom{3+3-1}{3} = \binom{5}{3} = 10$ terms. These are

$$x_1^3 + x_2^3 + x_3^3 + 3x_1^2x_2 + 3x_1x_2^2 + 3x_2^2x_3 + 3x_2x_3^2 + 3x_1^2x_3 + 3x_1x_3^2 + 6x_1x_2x_3.$$

4.9 Inclusion-exclusion principle

We saw that if A_1 and A_2 are disjoint finite sets, then $|A_1 \cup A_2| = |A_1| + |A_2|$. If A_1 and A_2 intersect, then $|A_1| + |A_2|$ counts the number of elements in $A_1 \cap A_2$ twice, so we must subtract off the number of elements in $A_1 \cap A_2$, hence we have the formula :

Inclusion-exclusion principle for two sets. If A_1, A_2 are two finite sets, then

$$|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2|.$$

Example 4.17. *How many integers from* 1 *to* 500 *are divisible by* 3 *or by* 7*?*

Solution. Let A be the set consisting in all integers from 1 to 500 which are divisible by 3. Consider B, the set of all integers from 1 to 500, divisible by 7. We have to find $|A \cup B|$. We write A and B as follows:

$$A = \{3k \mid 1 \leq 3k \leq 500\},$$
$$B = \{7l \mid 1 \leq 7l \leq 500\}.$$

In order to calculate $|A|$ we need to find the largest k such that $3k \leq 500$. This is 166, hence $|A| = 166$. In similar way, for $|B|$ we need to find the largest integer l with $7l \leq 500$ and we get $|B| = 71$.

Applying the inclusion-exclusion principle for two sets we have

$$|A \cup B| = |A| + |B| - |A \cap B| = 166 + 71 - |A \cap B| = 237 - |A \cap B|.$$

The set $A \cap B$ consists in all integers from 1 to 500 which are divisible by 3 and by 7, hence we can write

$$A \cap B = \{21s \mid 1 \leq 21s \leq 500\}$$

The largest s with property $21s \leq 500$ is 23, that is $|A \cap B| = 23$. Finally, it follows $|A \cup B| = 237 - |A \cap B| = 237 - 23 = 214$.

Inclusion-exclusion principle for three sets. If A_1, A_2, A_3 are finite sets, then

$$|A_1 \cup A_2 \cup A_3| = |A_1| + |A_2| + |A_3| - |A_1 \cap A_2| - |A_1 \cap A_3| - |A_2 \cap A_3| + |A_1 \cap A_2 \cap A_3|.$$

Example 4.18. *How many integers from* 1 *to* 2009 *are divisible by* 5 *or by* 7 *or by* 9 *?*

Solution. Let A be the set of integers from 1 to 2009 which are divisible by 5, B which are divisible by 7 and C which are divisible by 9. We have $5k \leq 2009$ is equivalent to $k \leq 401$, hence $|A| = 401$. Also, $7k \leq 2009$ is equivalent to $k \leq 287$, so $|B| = 281$. From $9k \leq 2009$, we get $k \leq 223$, that is $|C| = 223$.

In order to find $|A \cap B|$, observe that $35k \leq 2009$ is equivalent to $k \leq 57$. Also, $45k \leq 2009$, gives $k \leq 44$, and $63k \leq 2009$, gives $k \leq 31$. In this way we obtain $|A \cap B| = 57$, $|A \cap C| = 44$ and $|B \cap C| = 31$.

In order to find $|A \cap B \cap C|$, observe that $5 \cdot 7 \cdot 9k \leq 2009$ is equivalent to $k \leq 6$, hence $|A \cap B \cap C| = 6$.

Applying the inclusion-exclusion principle for three sets we get

$$\begin{aligned} |A \cap B \cap C| &= |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C| \\ &= 401 + 281 + 223 - 57 - 44 - 31 + 6 = 769. \end{aligned}$$

Theorem 4.17 (Inclusion-exclusion, general form). *If $A_1, A_2, \ldots, A_m$ are finite sets, then the following formula holds:*

$$\begin{aligned} |A_1 \cup A_2 \cup \cdots \cup A_m| = &\sum_{1 \leq i \leq m} |A_i| - \sum_{1 \leq i < j \leq m} |A_i \cap A_j| \\ &+ \sum_{1 \leq i < j < k \leq m} |A_i \cap A_j \cap A_k| + \cdots \\ &+ (-1)^m |A_1 \cap A_2 \cap \cdots \cap A_m|. \end{aligned}$$

Proof. Proceed by induction on m. For $m = 2$ and $m = 3$ the formula was proved in the previous particular cases. For the the induction step, just write

$$A_1 \cup A_2 \cup \cdots \cup A_m \cup A_{m+1} = (A_1 \cup A_2 \cup \cdots \cup A_m) \cup A_{m+1} = A \cup A_{m+1},$$

where $A = A_1 \cup A_2 \cup \cdots \cup A_m$. From inclusion-exclusion principle for two sets we obtain

$$|A_1 \cup A_2 \cup \cdots \cup A_m \cup A_{m+1}| = |A \cup A_{m+1}| = |A| + |A_{m+1}| - |A \cap A_{m+1}|,$$

then use $A \cap A_{m+1} = (A_1 \cap A_{m+1}) \cup (A_2 \cap A_{m+1}) \cup \cdots \cup (A_m \cap A_{m+1})$ and apply the induction hypothesis. Finally group the resulting terms. □

Euler's totient function. For any positive integer n denote by $\varphi(n)$ the number of integers m such that $m < n$ and $gcd(m, n) = 1$.

The arithmetic function φ is called **Euler's totient function**. Clearly, $\varphi(1) = 1$ and for any prime p we have $\varphi(p) = p - 1$. Moreover, if n is a positive integer such that $\varphi(n) = n - 1$, then n is a prime.

If $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, then we have the formula

$$\varphi(n) = n \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right).$$

For the proof we employ the inclusion-exclusion principle. For each index $i = 1, \ldots, k$ consider the set

$$T_i = \{d \mid d \leq n \text{ and } p_i | d\}.$$

It follows that

$$T_1 \cup \cdots \cup T_k = \{m \mid m \leq n \text{ and } \gcd(m,n) > 1\}.$$

Hence, we obtain

$$\begin{aligned}\varphi(n) &= n - |T_1 \cup \cdots \cup T_k| \\ &= n - \sum_{i=1}^{k} |T_i| + \sum_{1 \geq i < j \leq k} |T_i \cap T_j| - \cdots + (-1)^k |T_1 \cap \cdots \cap T_k|.\end{aligned}$$

On the other hand, we have

$$|T_i| = \frac{n}{p_i}, \quad |T_i \cap T_j| = \frac{n}{p_i p_j}, \quad \ldots, \quad |T_1 \cap \cdots \cap T_k| = \frac{n}{p_1 \cdots p_k}.$$

Finally,

$$\begin{aligned}\varphi(n) &= n - \sum_{i=1}^{k} \frac{n}{p_i} + \sum_{1 \geq i < j \leq k} \frac{n}{p_i p_j} - \cdots + (-1)^k \frac{n}{p_1 \cdots p_k} \\ &= n \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right),\end{aligned}$$

and the formula is proved.

The number of surjective functions. Let M and N be finite sets, and $m = |M|$ and $n = |N|$ their cardinalities. Counting the functions of the form $f \mid M \to N$ is easy. Each $x \in M$ has n choices for its image, the choices are independent, and therefore the number of functions is n^m. How many of these functions are surjective ? To answer this question, let $N = \{y_1, y_2, \ldots, y_n\}$ and let A_i be the set of functions in which y_i is not the image of any element in M. Writing A for the set of all functions and S for the set of all surjective functions, we have

$$S = A - (A_1 \cup \cdots \cup A_n).$$

We already know $|A|$. Similarly, $|A_i| = (n-1)^m$. Furthermore, the size of the intersection of k of the A_i is

$$|A_{i_1} \cap \cdots \cap A_{i_k}| = (n-k)^m.$$

We can now use inclusion-exclusion principle to get the number of functions in the union, namely,

$$|A_1 \cup \cdots \cup A_n| = \sum_{k=1}^{n} (-1)^{k+1} \binom{n}{k} (n-k)^m.$$

To get the number of surjective functions, we subtract the size of the union from the total number of functions

$$s_{m,n} = |S| = \sum_{k=0}^{n} (-1)^k \binom{n}{k} (n-k)^m.$$

For $m < n$, this number should be 0 , and for $m = n$, it should be $n!$.
Finally, we can write

$$s_{m,n} = \begin{cases} \sum_{k=0}^{n} (-1)^k \binom{n}{k} (n-k)^m \text{ if } m \geq n \\ n! \text{ if } m = n \\ 0 \text{ if } m < n \end{cases} \tag{4.3}$$

Derangements. Since the actual nature of the objects does not matter, we may take X to be the set $\{1,2,\cdots,n\}$ in which the location of each of the integers is that specified by its position in the sequence $1,2,\ldots,n$.

A **derangement** of $\{1,2,\ldots,n\}$ is a permutation $i_1 i_2 \cdots i_n$ of $\{1,2,\ldots,n\}$ with $i_1 \neq 1, i_2 \neq 2, \ldots, i_n \neq n$, i.e., a derangement of $\{1,2,\ldots,n\}$ is a permutation $i_1 i_2 \cdots i_n$ of $\{1,2,\ldots,n\}$ in which no integer occupies its natural position.

We denote the numbers of derangements of $\{1,2,\ldots,n\}$ by D_n. For $n = 1$, there is no derangement. For $n = 2$, there is only one derangement: 21. For $n = 3$, there are two derangements: 231 and 312. The derangements for $n = 4$ are 2143 ; 3142 ; 4123 ; 2341 ; 3412 ; 4312 ; 2413 ; 3421 ; 4321. Thus we have 9 derangements in this case. These examples show that

$$D_1 = 0;\ D_2 = 1;\ D_3 = 2;\ D_4 = 9.$$

For $n \geq 1$, the following formula holds true

$$D_n = n! \left(1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \cdots + \frac{(-1)^n}{n!}\right). \tag{4.4}$$

In order to prove formula (4.4), consider S to be the set of all $n!$ permutations of $\{1,2,\ldots,n\}$. For $j = 1,2,\ldots,n$, let P_j be the property that, in a permutation, j is in its natural position. A permutation of $\{1,2,\ldots,n\}$ is a derangement if it has none of properties $P_1, P_2, \ldots, P_n$. Denote by A_j the set of permutations of $\{1,2,\ldots,n\}$ with $P_j, j = 1,2,\ldots,n$. The derangements of $\{1,2,\ldots,n\}$ are precisely those permutations in $S \setminus (A_1 \cup A_2 \cdots \cup A_n)$. Hence

$$D_n = |S| - |A_1 \cup A_2 \cdots \cup A_n| = n! - |A_1 \cup A_2 \cdots \cup A_n|.$$

We now calculate $|A_1 \cup A_2 \cdots \cup A_n|$ by using inclusion-exclusion formula.

The permutations in A_1 have the form $1 i_2 \cdots i_n$, where $i_2 \cdots i_n$ is a permutation of the set $\{2,\ldots,n\}$. Thus $|A_1| = (n-1)!$.

In the same way, we have

$$|A_j| = (n-1)!.$$

The permutations in $A_1 \cap A_2$ are of the form $12i_3 \cdots i_n$, where $i_3 \cdots i_n$ is a permutation of $\{2,\ldots,n\}$. Thus $|A_1 \cap A_2| = (n-2)!$. Similarly,

$$|A_i \cap A_j| = (n-2)! \text{ for } i \neq j.$$

The permutations in $A_1 \cap A_2 \cap \cdots \cap A_k$ have the form $12\cdots k i_{k+1} \cdots i_n$ where $i_{k+1} \cdots i_n$ is a permutation of $\{f_{k+1},\ldots,n\}$. Thus $|A_1 \cap A_2 \cdots A_k| = (n-k)!$. A similar argument shows that

$$|A_{i_1} \cap A_{i_2} \cap \cdots \cap A_{i_k}| = (n-k)!$$

for any k-subset $\{i_1,i_2,\ldots,i_k\}$ of $\{1,2,\ldots,n\}$. Since there are $\binom{n}{k}$ k-subsets of $\{1,2,\ldots,n\}$, by the inclusion-exclusion principle, we have

$$\begin{aligned} D_n &= n! - \binom{n}{1}(n-1)! + \binom{n}{2}(n-2)! + \cdots + (-1)^n \binom{n}{n}(n-n)! \\ &= n! - \frac{n!}{1!} + \frac{n!}{2!} - \frac{n!}{3!} + \cdots (-1)^n \frac{n!}{n!} \\ &= n!\left(1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \cdots (-1)^n \frac{1}{n!}\right). \end{aligned}$$

Recall the Taylor series for the exponential function

$$e^x = \sum_{j=0}^{\infty} \frac{x^n}{n!}.$$

So we have

$$e^{-1} = 1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \frac{1}{4!} - \cdots$$

Therefore, for a fixed n, the probability to extract a derangement out of the $n!$ permutation is

$$\frac{D_n}{n!} = 1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \frac{1}{4!} - \cdots (-1)^n \frac{1}{n!}.$$

Notice that $\frac{D_n}{n!} \to \frac{1}{e}$ for $n \to \infty$.

The following recursive formulas for the number of derangements hold:

$$\begin{aligned} D_n &= nD_{n-1} + (-1)^n \\ D_n &= (n-1)(D_{n-2} + D_{n-1}), \quad n = 3,4,5,\ldots \end{aligned}$$

Example 4.19. *Let $A_1, A_2, \ldots, A_n$ be finite subsets of a set S. Denote by $d(n)$ the number of elements which appear in an odd number of subsets among $A_1, \ldots, A_n$. Show that for all $1 \leq k \leq n$, the number*

$$d(n) - \sum_{i=1}^{n} |A_i| + 2\sum_{i<j} |A_i \cap A_j| + \cdots + (-1)^k 2^{k-1} \sum_{i_1<\ldots<i_k} |A_{i_1} \cap A_{i_2} \cap \ldots \cap A_{i_k}|$$

is divisible by 2^k.

Solution. Let $S = A_1 \cup \ldots \cup A_n$ and, for any subset A of S we denote by 1_A its indicator function relative to S, namely $1_A : S \to \{0,1\}$ is given by

$$1_A(s) = \begin{cases} 1 \text{ if } s \in A \\ 0 \text{ otherwise} \end{cases}.$$

It is very easy to show that for any $A, B \subseteq S$, we have

- $1_{A\cap B} = 1_A \cdot 1_B$;
- $1_{A\cup B} = 1_A + 1_B - 1_A \cdot 1_B$;
- $1_{S\setminus A} = 1 - 1_A$;
- $A \subset B$ if and only if a $1_A(s) \leq 1_B(s)$for all $s \in S$;
- If $|A| < \infty$, then $|A| = \sum_{s\in S} 1_A(s)$.

Returning to our problem, note that it is sufficient to prove the result for $k = n$. For each $x \in S$ let P_x be 1 if x belongs to an odd number of A_i 's and 0 otherwise. It suffices to prove that for all $x \in S$ we have

$$P_x - \sum_{i=1}^{n} 1_{x\in A_i} + \cdots + (-1)^n 2^{n-1} 1_{x\in A_1\cap\ldots\cap A_n} \equiv 0 \pmod{2^n},$$

as then the result follows by summing over all $x \in S$. On the other hand,

$$\sum_{i=1}^{n} 1_{x\in A_i} - \cdots + (-1)^{n-1} 2^{n-1} 1_{x\in A_1} \cdot \ldots \cdot 1_{x\in A_n}$$

is equal to

$$\frac{1 - (1 - 2 \cdot 1_{x\in A_1}) \cdots (1 - 2 \cdot 1_{x\in A_n})}{2} = \frac{1 - (-1)^k}{2}$$

where k is the number of A_i 's containing x. The result follows.

Let us now see an example given at the 2012 Tuymaada Olympiad. This was regarded as the hardest problem in the competition.

Example 4.20. 25 *little donkeys stand in a row; the rightmost of them is Eeyore. Winnie-the-Pooh wants to give a balloon of one of the seven colors of the rainbow to each donkey, so that successive donkeys receive balloons of different colors, and so that at least one balloon of each color is given to some donkey. Eeyore wants to give*

to each of the 24 *remaining donkeys a pot of one of six colors of the rainbow (except red), so that at least one pot of each color is given to some donkey (but successive donkeys can receive pots of the same color). Which of the two friends has more ways to get his plan implemented, and how many times more?*

Solution. In fact both these numbers can be computed. Label the colors of the rainbow by 1,2,3,4,5,6,7, with red being the 7th. Denote by A_k, $1 \le k \le 7$, the set of ways to give balloons of any but the k-th color to 25 donkeys, so that neighboring donkeys receive balloons of different color (though maybe not all 6 of the available colours are being used). Clearly, for any $K \subseteq \{1,2,3,4,5,6,7\}$, we have $|\bigcap_{k\in K} A_k| = (7-|K|)(6-|K|)^{24}$. By the Principle of Inclusion/Exclusion (PIE) we have

$$\left|\bigcup_{k=1}^{7} A_k\right| = \sum_{\ell=1}^{7}(-1)^{\ell-1}\sum_{|K|=\ell}\left|\bigcap_{k\in K} A_k\right| = \sum_{m=0}^{6}(-1)^m\binom{7}{m}m(m-1)^{24}.$$

Now, denote by A_0 the set of ways to give balloons of any of the colors of the rainbow to 25 donkeys, so that neighboring donkeys receive balloons of different color (though maybe not all 7 of the available colors are being used). Clearly $|A_0| = 7\cdot 6^{24}$. The number we are looking for, the number of such ways that use all 7 colors, is therefore

$$|A_0| - \left|\bigcup_{k=1}^{7} A_k\right| = \sum_{m=0}^{7}(-1)^{m-1}\binom{7}{m}m(m-1)^{24}$$

We have now to compute the number of ways to distribute pots, i.e. 6 colors (no red), 24 donkeys, no restriction for neighboring donkeys, but all 6 colors to be used. Denote, following the fashion of above, by B_k, $1 \le k \le 6$, the set of ways to give pots of any but red and the k-th color to 24 donkeys (though maybe not all 5 of the available colors are being used). Clearly, for any $K \subseteq \{1,2,3,4,5,6\}$, we have $|\bigcap_{k\in K} B_k| = (6-|K|)^{24}$. By the Principle of Inclusion/Exclusion (PIE) we have

$$\left|\bigcup_{k=1}^{6} B_k\right| = \sum_{\ell=1}^{6}(-1)^{\ell-1}\sum_{|K|=\ell}\left|\bigcap_{k\in K} B_k\right| = \sum_{m=0}^{5}(-1)^{m-1}\binom{6}{m}m^{24}.$$

Now, denote by B_0 the set of ways to give pots of any of the colors of the rainbow but red to 24 donkeys (though maybe not all 6 of the available colors are being used). Clearly $|B_0| = 6^{24}$. The number we are looking for, the number of such ways that use all 6 colors, is therefore

$$|B_0| - \left|\bigcup_{k=1}^{6} B_k\right| = \sum_{m=0}^{6}(-1)^{m}\binom{6}{m}m^{24}$$

All it remains is to notice that, term by term,

$$\sum_{m=1}^{7}(-1)^{m-1}\binom{7}{m}m(m-1)^{24}=7\sum_{m=0}^{6}(-1)^{m}\binom{6}{m}m^{24}$$

so there are 7 more ways to distribute balloons than pots.

Alternative solution. We present another official, i.e. presented on the marking scheme, for this problem. This method does not actually count the ways, but rather establishes a one-to-one correspondence between Eeyore's ways to distribute pots and Winnie's ways to distribute balloons, all the while giving Eeyore a red one. We present it because it anticipates the concepts discussed in the next section.

Concretely, pots and balloons have the same color, except when a pair of two consecutive pots share a same color, in which case the color of the second balloon in the pair is red.

Now, the total number of ways Winnie can distribute balloons is 7 times larger, since the balloon given to Eeyore may be of any of the 7 colors, not just red, and clearly for each of the colors of the balloon given to Eeyore there are a same number of ways to do it.

4.10 Counting by a bijection

This is a basic method of counting which is very useful in many concrete problems. We first revisit some results given earlier in Section 4.1.

Let A and B be two sets. A function $f : A \to B$ is called:

- **one-to-one** or **injective** if for all $a,b \in A$ we have $f(a) = f(b) \Rightarrow a = b$.
- **onto** or **surjective** if for all $b \in B$ there exists an $a \in A$ such that $f(a) = b$.
- **bijective** if the function is one-to-one and onto.

The following properties of injective, surjective and bijective functions are relevant for counting problems:

- If there is an **injective** function $f : A \to B$, then $|A| \leq |B|$.
- If there is a **surjective** function $f : A \to B$, then $|A| \geq |B|$.
- If there is a **bijective** function $f : A \to B$, then $|A| = |B|$.

The key point of the last property is that whenever counting the number of objects in a given set A presents a challenge, an alternative is to establish a bijection between A and another set B whose cardinal is easier to find.

If a bijection $f : A \to B$ exists, then there is also a bijection $g : B \to A$. Here we provide some classical examples of counting with bijections.

Example 4.21. *Let m,n be positive integers. How many increasing functions $f : \{1,2,\ldots,n\} \to \{1,2,\ldots,m\}$ can one define?*

Solution. Denote the following sets of functions:

$$A = \{f : \{1,2,\ldots,n\} \to \{1,2,\ldots,m\}, \quad f \text{ is increasing}\}$$
$$B = \{g : \{1,2,\ldots,n\} \to \{1,2,\ldots,m\}, \quad g \text{ is strictly increasing}\}.$$

The function $h : A \to B$ defined by $h(f(i)) = f(i) + i - 1 = g(i)$, $i = 1,\ldots,n$ is a bijection between A and B, and clearly, $|B| = \binom{n+m-1}{m}$.

Example 4.22. *In a single-elimination tournament there are n people competing. How many matches are needed to decide the champion?*

Solution. There is a bijection between the set of eliminated players and the set of matches played. To decide the single winner, $n-1$ players must be eliminated, therefore $n-1$ are required for deciding the champion.

Example 4.23. *A set S of integers is called **fat** if each of its elements is greater or equal to $|S|$. For example, the empty set, or the set $\{5,6,7,8\}$ are fat, while the set $\{1,2,3\}$ is not. Establish a recursion for the sequence $(f_n)_{n=0}^{\infty}$, where f_n is the number of fat subsets of $\{1,\ldots,n\}$.*

Solution. We split the subsets of $\{1,2,\ldots,n+1\}$ into those which contain $n+1$, and those who do not (whose number is actually f_n, as they are in fact fat subsets of $\{1,\ldots,n\}$.)

The number of fat subsets containing $n+1$ are in a bijective correspondence with the fat subsets of $\{1,2,\ldots,n-1\}$, through the mapping $\{x_1,x_2,\ldots,x_k,n+1\} \mapsto \{x_1-1,x_2-1\ldots,x_k-1\}$, where $x_1 < x_2 < \cdots < x_k$. It follows that there are f_{n-1} fat subsets of $\{1,\ldots,n+1\}$ which contain $n+1$, hence the desired recurrence relation is

$$f_{n+1} = f_n + f_{n-1}, \quad n \geq 2,$$

where $f_1 = 2$ (fat sets: $\emptyset$ and $\{1\}$) and $f_2 = 3$ (fat sets: $\emptyset$, $\{1\}$ and $\{2\}$). Clearly, the fat sets for $n = 3$ are $\emptyset$, $\{1\}$, $\{2\}$, $\{3\}$ and $\{2,3\}$, hence $f_3 = 5$. Notice that $f_n = F_{n+2}$, $n \geq 1$, where $(F_n)_{n\geq 0}$ is the Fibonacci sequence.

Example 4.24. *Let m, n be positive integers, and consider an $m \times n$ rectangular grid. How many paths are there from $(0,0)$ to (m,n), following the grid lines and only moving up or right?*

Solution. Each path from $(0,0)$ to (m,n) following the grid lines and only moving up or right consists of exactly $n+m$ segments, being uniquely defined by the position of n vertical steps (the other m being horizontal steps). Hence, the set of such paths is in a bijective correspondence with the subsets of $\{1,2,\ldots,m+n\}$ with n elements, so the answer is $\binom{n+m}{n} = \binom{n+m}{m}$.

Example 4.25 (Catalan numbers). *Prove that the number of lattice paths from the point $(0,0)$ to (n,n) following the grid lines, located lower than, or on the bisector line $y=x$ is $C_n=\dfrac{1}{n+1}\binom{2n}{n}$.*

These numbers recover the Catalan sequence $(C_n)_{n\geq 0}$ (A000108 in OEIS [211]), and starting with $1,1,2,5,14,42,132,429,1430,4862,16796,58786,\ldots$.

Solution. First, notice that each path going from $(0,0)$ to (n,n) contains n steps to the right, and n steps upwards. For each such path going above the diagonal we associate another path, as follows:
1) keep all steps until going above the diagonal for the first time unchanged;
2) swap all remaining steps (right become up, up become right).
If the first point reached above the diagonal is $(k,k+1)$, then the initial path contained $k+(n-k)=n$ steps to the right, and $(k+1)+(n-k-1)=n$ steps upwards. The new path will then have $k+(n-k-1)=n-1$ steps to the right and $(k+1)+(n-k)=n+1$ steps upwards, hence it will end at $(n-1,n+1)$. This mapping is well defined and bijective, so the number of lattice paths from $(0,0)$ to (n,n) not going above the diagonal, is actually equal to the total number of paths from $(0,0)$ to $(n-1,n+1)$. Therefore

$$C_n=\binom{2n}{n}-\binom{2n}{n+1}=\frac{1}{n+1}\binom{2n}{n}.$$

Example 4.26. *A triangular grid is obtained by tiling an equilateral triangle of side length n by n^2 equilateral triangles of side length 1, whose sides are parallel to the big triangle. Determine the number of*

1) rhombi of side length 1.
2) parallelograms.

Solution. 1) Each short lattice segment within the triangle, can be the diagonal of exactly one rhombus (so there is a bijection between the two sets), hence the answer is

$$3(1+\cdots+n-1)=3\frac{n(n-1)}{2},$$

as each of the sides of the big triangles has n segments of length 1, which are discounted from the total count.

2) A parallelogram has the sides parallel to the sides of the original triangle. One may notice that extending the sides of the parallelogram, they intersect the a line parallel to the third side and having $n+1$ segments (hence $n+2$ points) in 4 points. This shift of one position is to allow one to count the parallelograms having one vertex on the non-parallel line. The set of parallelograms and the set of quadruples selected from amongst these $n+2$ points on the line are in bijective correspondence, so the number of parallelograms (accounting for each of the 3 orientations) is $3\binom{n+2}{4}$.

Example 4.27. *Here we have other examples related to the Catalan sequence.*

1) Prove that the number of expressions containing n pairs of correctly matched brackets is C_n. For $n = 3$, the correctly matched brackets are

$$()()(), \quad ()(()), \quad (())(), \quad (()()), \quad ((())).$$

2) Prove that the number of increasing functions $f : \{1,\dots,n\} \to \{1,\dots,n\}$ with the property $f(x) \leq x$, $x = 1,\dots,n$ is C_n.
3) Show that the number of sequences $(a_1,\dots,a_{2n+1})$ with nonnegative terms such that $a_1 = a_{2n+1} = 0$ and $|a_i - a_{i+1}| = 1$ for $i = 1,\dots,2n$ is C_n.
4) Prove that C_n satisfies the recurrence relation

$$C_n = C_{n-1}C_0 + C_{n-2}C_1 + \cdots + C_1C_{n-1} + C_0C_{n-1}.$$

Solution. 1) The valid bracket combinations can be put in bijective correspondence with the paths in Example 4.25, associating the "(" brackets with steps to the right, and the ")" brackets with steps upwards.

2) We associate each function $f : \{1,\dots,n\} \to \{1,\dots,n\}$ satisfying $f(x) \leq x$ for $x = 1,\dots,n$ with the Catalan path having the highest point in column $i-1$ equal to $(i-1, f(i)-1)$, $i = 2,\dots,n$.

3) The paths in Example 4.25, can be put in a bijective correspondence with a sequence, by associating a number a_i, $i \geq 2$ with a step to the right if $a_{i-1} < a_i$ and with a step upwards otherwise.

4) One can count the Catalan paths based on the first point reached on the diagonal, after $(0,0)$. If the first point of the path on the diagonal is (k,k), $k = 1,\dots,n$, then the number of paths from $(0,0)$ to (k,k) with this property is the number of Catalan paths from $(1,0)$ to $(k,k-1)$ (as the first segment is horizontal, while the last one is vertical), that is C_{k-1}, with $C_0 = 1$. Once (k,k) is reached, the number of Catalan paths from (k,k) to (n,n) is C_{n-k}, hence we have exactly $C_{k-1}C_{n-k}$ paths hitting the diagonal first time at the point (k,k), $k = 1,\dots,n$. Summing over $k = 1,\dots,n$ we obtain the formula.

Example 4.28. *Consider the permutations $(x_1,x_2,\dots,x_{2n})$ of set $\{1,2,\dots,2n\}$. Determine if the number of permutations having the property $|x_i - x_{i+1}| = n$ for at least one value $i \in \{1,\dots,2n-1\}$, is greater then the number of permutations which do not have this property.*

Solution. Let us call two numbers $x,y \in \{1,2,\dots,2n\}$ twins if $|x-y| = n$, and a permutation $(x_1,x_2,\dots,x_{2n})$ of this set will be called of type T_k if there are exactly k pairs of twins, i.e., there are exactly k indices i with the property $|x_i - x_{i+1}| = n$. Let us define the mapping $f : T_0 \to T_1$ as follows. If $(x_1,x_2,\dots,x_{2n}) \in T_0$ and x_k, $k > 2$ is the twin of x_1, then

$$f(x_1,x_2,\dots,x_{2n}) = (x_2,\dots,x_{k-1},x_1,x_k,\dots,x_{2n}).$$

Notice that the mapping is injective but not surjective, hence the number of permutations with at least one pair of neighbouring twins is greater than the number of permutations without pairs of neighboring twins.

Example 4.29. *Prove that the number of subsets with k elements of $\{1,\ldots,n\}$, in which no numbers are consecutive is $\binom{n-k+1}{k}$.*

Solution. We associate the subsets of $S \subseteq \{1,\ldots,n\}$ with binary words $a_1a_2\ldots a_n$ for which $a_i = 1$ whenever $i \in S$ and $a_i = 0$ otherwise. A set S having no consecutive integers is represented by a binary word with no consecutive 1's, hence there is a bijection between them and the number of words having k values equal to 1, $n-k$ values equal to 0, and no consecutive 1's. To compute the cardinal of this set, we label the $n-k$ digits equal to 0 from 1 to $n-k$. Between them we have to add k digits 1, avoiding consecutive 1's. Hence, each digit 1 is preceded by a 0 digit, indicated by it's label $0,\ldots,n-k$ (this can be 0 as well, when the word starts with 1). This can be done in exactly $\binom{n-k+1}{k}$ ways, which ends the proof.

Example 4.30. *Three people A, B, C play the following game: for a fixed positive integer $k \leq 2022$, a subset of $\{1,2,\ldots,2022\}$ with k elements is randomly chosen, with an equal probability of each choice. The winner is decided based on the reminder of the sum of the chosen numbers when divided by 3: A for 0, B for 1 and C for 2. For which values k is the game fair, and who has the best odds when it is not?*

Solution. Let us split the set $\{1,2,\ldots,2022\}$ into sets $X_j = \{3j-2, 3j-1, 3j\}$, $j = 1,\ldots,674$. Denote by $\mathcal{F}$ the family of all subsets $Y \subseteq \{1,2,\ldots,2022\}$ with k elements with the property $|Y \cap X_j| = 1$ or $|Y \cap X_j| = 2$ for some j.

Let j_0 be the smallest such j, and define Y' as the set with k elements obtained by replacing in Y the elements in $Y \cap X_{j_0}$ with the ones following cyclically inside X_{j_0} (i.e., shifting to the right adds 1 to the sum in the first case, or 2 in the second case). Applying this process to Y', we obtain the set Y'', and applying again to Y'' we get Y'''. Denoting by $s(Y)$ the modulo 3 sum of the elements in set Y, one can check that $s(Y)$, $s(Y')$ and $s(Y'')$ are distinct, while $Y''' = Y$. Thus, this operator $'$ gives a bijective correspondence between the three families $\mathcal{P}_0, \mathcal{P}_1, \mathcal{P}_2 \subseteq \mathcal{F}$ for with the property $s(P_0) = 0$ for $P_0 \in \mathcal{P}_0$, $s(P_1) = 1$ for $P_1 \in \mathcal{P}_1$, and $s(P_2) = 2$ for $P_2 \in \mathcal{P}_2$.

When $k \pmod 3 = 0$, then the elements not belonging to $\mathcal{F}$ are those formed of unions of several triads. As the sum of elements in each such triad is divisible by 3, then player A has the advantage. For $k \pmod 3 \neq 0$, each set B with k elements belongs to $\mathcal{F}$, hence the game is fair.

Example 4.31. *Let k and n be positive integers. Denote by A the set of all sequences $a = (a_1,\ldots,a_k)$ whose integer entries satisfy $0 \leq a_i \leq n$, $i = 1,\ldots,k$. If $m(a) = \min\{a_1,a_2,\ldots,a_k\}$ and $M(a) = \max\{a_1,a_2,\ldots,a_k\}$, show that*

$$\sum_{a\in A} (m(a) + M(a)) = n\,(n+1)^k.$$

Solution. Clearly, $|A| = (n+1)^k$. To each sequence $a = (a_1, a_2, \ldots, a_k)$ we can associate the sequence $a' = (n - a_1, n - a_2, \ldots, n - a_k)$, through a bijective correspondence between A and A. Since $M(a') = n - m(a)$, one obtains

$$\begin{aligned}\sum_{a\in A}(m(a)+M(a)) &= \sum_{a\in A} m(a) + \sum_{a'\in A} M(a') \\ &= \sum_{a\in A} m(a) + \sum_{a\in A}[n - m(a)] = n|A| = n\,(n+1)^k.\end{aligned}$$

Example 4.32. *Let $1 \le k \le n$ be positive integers. For each subset of $\{1,2,\ldots,n\}$ with k elements, we consider the minimal element. Prove that the arithmetic mean of these minima is $\frac{n+1}{k+1}$.*

Solution. The set A of $\{1,2,\ldots,n\}$ with k elements indexed as $(a_1,\ldots,a_k)$ with $1 \le a_1 < a_2 < \cdots < a_k \le n$ are in bijective correspondence with the set B containing the sets $(b_1,\ldots,b_{k+1})$ with $k+1$ elements, having the sum $n+1$. This bijection can be defined by the formula

$$(a_1,\ldots,a_k) \mapsto (a_1, a_2 - a_1, \ldots, a_k - a_{k-1}, n+1-a_k).$$

The problem reduces to computing the aritmetic mean of b_1, over all configurations $(b_1,\ldots,b_{k+1})$ having the sum $n+1$. Notice that the elements in this $(k+1)$-tuple can be permuted, hence the arithmetic mean of b_1 is also equal to the arithmetic mean of b_j, $j = 1,\ldots,k+1$. One obtains

$$\frac{1}{(k+1)\,|B|}\sum_{(b_1,\ldots,b_{k+1})\in B}(b_1+\cdots+b_{k+1})\frac{(n+1)\,|B|}{(k+1)\,|B|} = \frac{n+1}{k+1}.$$

4.11 Counting in two ways

This is a specific method in combinatorics. Here are a few examples.

Example 4.33. *Prove the following identities:*

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

2) $\binom{a+b}{n} = \sum_{k=0}^{n}\binom{a}{k}\binom{b}{n-k}$ *(Vandermonde).*

3) $\binom{n}{k}\binom{k}{m} = \binom{n}{m}\binom{n-m}{k-m}$, *where $n \ge k \ge m$ are integers.*

4) $\sum_{k=0}^{m}\binom{m}{k}\binom{n+k}{m} = \sum_{k=0}^{m}\binom{m}{k}\binom{n}{k}2^k$.

Solution. 1) Let us label a set of n objects by $O_1, O_2, \ldots, O_n$. Clearly, $\binom{n}{k}$ is the number of ways of selecting k objects out of n. For each value of k, we have two mutually exclusive possibilities. Either O_n is taken, in which case the remaining $k-1$ objects can be chosen in $\binom{n-1}{k-1}$ ways, or O_n is not taken, when the k objects can be chosen in $\binom{n-1}{k}$ ways. This confirms the identity.

2) Let A and B be two disjoint sets with cardinals $|A| = a$ and $|B| = b$. With these notations, the expression on the left represents the ways of choosing a subset $X \subseteq A \cup B$ having n elements. We are now summing over all possible intersections $X \cap A$ and $X \cap B$. The intersection $X \cap A$ may have $k = 0, \ldots, n$ elements, and since the sets A, B are disjoint, one must have $|X \cap B| = n - k$. For each value of $k = 0, \ldots, n$, there will be $\binom{a}{k}$ ways to select the set $X \cap A$, and $\binom{b}{n-k}$ ways to select the elements in $X \cap B$. We notice that in certain cases, some of terms in the right-hand side will may be equal to zero.

3) We first notice that unless $m \leq k \leq n$, the identity holds trivially with both side equal to zero. Let A be a set with n elements. For given integers $m \leq k \leq n$, the left-hand side corresponds to the number of choices for a pair of subsets (B, C) with the properties $|B| = k$, $|C| = m$ and $C \subseteq B \subseteq A$. Clearly, B can be chosen in $\binom{n}{k}$ ways, while C can be chosen in $\binom{k}{m}$ distinct ways.

The right-hand side also counts the pair of subsets (B, C) with the properties $|B| = k$, $|C| = m$ and $C \subseteq B \subseteq A$, but now first choosing the set $C \subseteq A$, possible in $\binom{n}{m}$. Apart from the m elements from C, the set $B \setminus C$ has other $k - m$ other elements, which are selected from the remaining $n - m$ elements of $A \setminus C$, for a total of $\binom{n-m}{k-m}$ choices.

4) To count the right-hand side one may consider two disjoint sets A and B with cardinals $|A| = m$ and $|B| = n$.

For a fixed positive integer k, the number of pairs of sets (X, Y) having cardinals $|X| = k$ and $|Y| = m$, satisfying $X \subseteq A$ and $Y \subseteq B \cup X$ is given by $\binom{m}{k}\binom{n+k}{m}$. Summing over all $k = 0, \ldots, m$ the left-hand side expression represents the number of pairs (X, Y) satisfying $X \subseteq A$ and $Y \subseteq B \cup X$ and $|Y| = m$.

These pairs can be placed in bijective correspondence with the triples $(Y \cap B, Y \cap A, X \setminus Y)$, satisfying $X \subseteq A$ and $Y \subseteq B \cup X$ and $|Y| = m$. These can be counted by first choosing $Y \cap B$, then $Y \cap A$ and finally X. When $|Y \cap B| = k$ there are $\binom{n}{k}$ choices for $Y \cap B$, $\binom{m}{m-k}$ choices for $Y \cap A$ and 2^k choices for $Y \setminus X$ (as each of the k elements in $A \setminus Y$ may belong, or not to X). Summing over all values of k we obtain the desired result.

Example 4.34. *Let n be a positive integer. Prove that*

$$\tau(1) + \tau(2) + \cdots + \tau(n) = \left\lfloor \frac{n}{1} \right\rfloor + \left\lfloor \frac{n}{2} \right\rfloor + \cdots + \left\lfloor \frac{n}{n} \right\rfloor,$$

where $\tau(k)$ represents the number of divisors of the positive integer k.

Solution. Both sums represent the number of pairs (a,b) of positive integers satisfying $a \mid b$ and $b \leq n$. When fixing a first one obtains the right-hand side, while fixing b first, the left-hand side is obtained.

Example 4.35. *Let S be a set of n persons such that:*

1. each person has exactly k friends in S;
2. any two friends have exactly l common friends in S;
3. any two persons who are not friends, have exactly m common friends.

Prove that $m(n-k) - k(k-l) + k - m = 0$.

Solution. Consider an arbitrary person P in S. By property 1., P has k friends (denote this set by A) and $n-k-1$ it does not know (we denote this set by B). We are now counting the pairs (P_1, P_2) with $P_1 \in A$ and $P_2 \in B$ for which P_1 and P_2 are friends. As a person $P_2 \in B$ is not a friend of P, the persons P_2 and P have m common friends (by 3.). Clearly, all these common friends belong to A, because P has no friends in B, P_2 is friends with exactly m persons in A. Since P_2 can be selected in exactly $n-k-1$ ways, we have $(n-k-1)m$ pairs (P_1, P_2) with $P_1 \in A$, $P_2 \in B$ in which P_1 and P_2 are friends.

Similarly, a person $P_1 \in A$ who is friend with P has l common friends with P (by 2.), all belonging to A. Since P_1 has a total of k friends (including P), he has exactly $k-l-1$ friends in B. Therefore, the number of pairs (P_1, P_2) with $P_1 \in A$, $P_2 \in B$ in which P_1 and P_2 are friends is exactly $k(k-l-1)$.

We conclude that $m(n-k-1) = k(k-l-1)$, which ends the proof.

Example 4.36. *Prove the following identities:*

1) $\displaystyle\sum_{k=0}^{n} \binom{n}{k} = 2^n.$

2) $\displaystyle\binom{n}{k} = \frac{n}{k}\binom{n-1}{k-1}.$

3) $\displaystyle\sum_{k=0}^{m} \binom{n}{k}\binom{n-k}{m-k} = 2^m \binom{n}{m}.$

4) $\displaystyle\sum_{k=0}^{n} k\binom{n}{k}^2 = n\binom{2n-1}{n-1}.$

5) $\displaystyle\sum_{p=k-3}^{n-3} \binom{p}{k-3}\binom{n-p-1}{2} = \binom{n}{k}.$

6) $\displaystyle\sum_{k\geq 0} \binom{p}{k}\binom{q}{k}\binom{k}{j} = \binom{q}{j}\binom{p+q-j}{q}.$

7) $\displaystyle\sum_{j\geq 0} \binom{n}{p+q-j}\binom{q}{j}\binom{p+q-j}{q} = \binom{n}{p}\binom{n}{q}.$

Solution. 1) The right-hand side is the number of subsets Y of a set X with n elements (as each of the n elements of X may belong to Y or not). The left-hand side counts the same sets, but splitting them by cardinal, where we have: $\binom{n}{k}$ sets with exactly k elements, where $k = 0, \ldots, n$.

2) Notice that this identity is equivalent to

$$k\binom{n}{k} = n\binom{n-1}{k-1}.$$

On the left we have the number of ways to select a group of k people out of n, and then designate one with a special role (i.e., the boss). On the right side we count the same thing, but first selecting the boss (in n ways), then its other $k-1$ companions, out of the $n-1$ persons left in the group.

3) First notice that for $n < m$ both sides vanish. Consider a set X with n elements. Both sides count the number of pairs of subsets (Y, Z) such that $Z \subseteq Y \subseteq X$ with $|Y| = m$ fixed, in two ways. Notice that the set Z can have $k = 0, \ldots, m$ elements. On the left, for every $k = 0, \ldots, m$, the set Z can be chosen in $\binom{n}{k}$ ways, while the other elements in $Y \setminus Z$ can be selected in $\binom{n-k}{m-k}$ ways. On the other hand, on the right-hand one can first choose the set Y in $\binom{n}{m}$ ways, which has 2^m subsets Z of cardinal $k = 0, \ldots, m$.

4) For the right-hand side one may use two disjoint sets A and B with the same cardinal n. Then, the number of ways of choosing an element $x \in A$ and then $n-1$ other elements from $(A \cup B) \setminus \{x\}$ is exactly $n\binom{2n-1}{n-1}$. Hence, on the right-hand side we counted the number of pairs (x, X) with the property $x \in A$, $X \subseteq (A \cup B) \setminus \{x\}$ and $|X| = n-1$. These pairs are in bijective correspondence with the triples (x, Y, Z), where $x \in Y \subseteq A$, $Z \subseteq B$ and $|Y \cup Z| = n$. To count them we first choose the set Y of cardinal $k = 0, \ldots, n$, then x, and finally Z, to obtain $k\binom{n}{k}\binom{n}{n-k}$ acceptable configurations. The total number is then $\sum_{k=0}^{n} k\binom{n}{k}\binom{n}{n-k}$, which ends the proof.

5) First, the number of subsets $X = \{x_1, \ldots, x_k\}$ with $x_1 < x_2 \cdots < x_k$ with k elements taken from a set with n elements is $\binom{n}{k}$. Since the values taken by x_{k-2} are in the range $k-2, \ldots, n-2$, for each $j = k-2, \ldots, n-2$, the number of choices for the set $\{x_1, \ldots, x_{k-3}\}$ is $\binom{j-1}{k-3}$ while the number of choices for the set $\{x_{k-1}, x_k\}$ is $\binom{n-j}{2}$. The identity is obtained by summing over the values $j = k-2, \ldots, n-2$ and then setting $p = j-1$.

6) Consider two disjoint sets A and B of cardinals $|A| = p$ and $|B| = q$. On the left-hand side we count the triples (X, Y, Z) such that $X \subseteq A$, $Y \subseteq B$, $Z \subseteq B \setminus Y$ with $|Z| = j$ and $|X \cup Y| = q$. To obtain the identity we sum over $k = 0, \ldots, p+q$ and use $\binom{q}{q-k} = \binom{q}{k}$. Notice that these triples are in bijective correspondence with the pairs (T, U) satisfying $U \subseteq B$, $T \subseteq (A \cup B) \setminus U$, $|U| = j$ and $|T| = p+q-j$, whose number is clearly $\binom{q}{j}\binom{p+q-j}{q}$.

7) Let A be a set with $|A| = n$. The number of pairs of sets $(X, Y) \subseteq A \times A$ such that $|X| = p$ and $|Y| = q$ is $\binom{n}{p}\binom{n}{q}$. These pairs are in a bijective correspondence with the triples (T, U, V) with the property $T \subseteq A$, $U \subseteq T$, $V \subseteq U$, $|U| = q$ and $|V \cup (T \setminus U)| = p$, through the map $(X, Y) \mapsto (X \cup Y, Y, X \cap Y)$. One can now count these triples by summing over all cardinals of $|V| = j$.

Example 4.37. *Compute the following sums:*

$$1^\circ \quad \sum_{k=0}^{n} (2k-1)\binom{n}{k}.$$

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

Solution. 1° We have shown that $\sum_{k=0}^{n}\binom{n}{k} = 2^n$ and now we compute

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

Notice that this is the number of ways of choosing a subset Y from of a set X with n persons, having a special element (the "boss"). This is the number of ordered pairs (y, Y), where $y \in Y \subseteq X$. Clearly, this number is $n2^{n-1}$, as y can be chosen in n ways, and each of the remaining $n-1$ elements in X may belong to Y, or not. The desired number is then $2 \cdot n2^{n-1} - 2^n = (n-1)\,2^n$.

2° One may easily notice that

$$\sum_{k=0}^{n} k^2\binom{n}{k} = \sum_{k=0}^{n} k(k-1)\binom{n}{k} + \sum_{k=0}^{n} k\binom{n}{k}.$$

Reasoning as above, consider a set X with n elements of which y_1, y_2 have special role. To compute $\sum_{k=0}^{n} k(k-1)\binom{n}{k}$ we may notice that this is the sum of ordered pairs (y_1, y_2, Y) such that $y_1, y_2 \in Y \subseteq X$, $y_1 \neq y_2$. This number is $n(n-1)2^{n-2}$, hence the desired sum is $n(n-1)2^{n-2} + n2^{n-1}$.

Example 4.38. *Let p and q be relatively prime positive integers. Prove that*

$$\left\lfloor \frac{p}{q} \right\rfloor + \left\lfloor \frac{2p}{q} \right\rfloor + \cdots + \left\lfloor \frac{(q-1)p}{q} \right\rfloor = \left\lfloor \frac{q}{p} \right\rfloor + \left\lfloor \frac{2q}{p} \right\rfloor + \cdots + \left\lfloor \frac{(p-1)q}{p} \right\rfloor.$$

Solution. Both sums represent the number of lattice points within the triangle determined by the lines $y = 0$, $x = q$ and $py = qx$. On the left-hand side, the points are counted horizontally, while on the right-hand side vertically.

Example 4.39. *Let m, n and $a_1 \leq a_2 \leq \cdots \leq a_n = m$ be positive integers. Denoting by b_k the number of elements a_i such that $a_i \geq k$, show that*

$$a_1 + a_2 + \cdots + a_n = b_1 + b_2 + \cdots + b_m.$$

Solution. Imagine the following diagram: n lines of points, and on the line i consider put a_i points. Counting the points horizontally (first count the points on each line, then add the results), one gets $a_1 + \cdots + a_n$. Second, counting the points vertically (first count the points on a column and then adding the results), one obtains the desired relation.

Example 4.40. *Let n be a positive integer. Prove that*

$$\sigma(1) + \sigma(2) + \cdots + \sigma(n) = \left\lfloor \frac{n}{1} \right\rfloor + 2\left\lfloor \frac{n}{2} \right\rfloor + \cdots + n\left\lfloor \frac{n}{n} \right\rfloor,$$

where $\sigma(k)$ represents the sum of divisors of the positive integer k.

Solution. Both sums represent the number of triples (a,b,c) of positive integers satisfying $a \leq b$ $b \mid c$ and $c \leq n$. Fixing b first one obtains the right-hand side, while fixing c first, the left-hand side is obtained.

Example 4.41. *Let n be a positive integer. Prove that*

$$1^2 + 2^2 + \cdots + n^2 = \binom{n+1}{2} + 2\binom{n+1}{3} = \frac{n(n+1)(2n+1)}{6}.$$

Solution. $1^2 + 2^2 + \cdots + n^2$ is the number of triples (x,y,z) of positive integers satisfying $x < z$, $y < z$ and $z < n+1$. We now count these in two different ways. First, the number of such triples for which $x < z$ is $\binom{n+1}{2}$ (one can choose 2 integers $\{1,\ldots,n+1\}$ and select $x = y$ as the smaller one, and z the bigger one), and the number of triples for which $x \neq z$ is $2\binom{n+1}{3}$ (for each triple (a,b,c) with the property $1 \leq a < b < c \leq n+1$ there are two triples (x,y,z), given by (a,b,c) and (b,a,c)).

Example 4.42. *In a finite sequence of real numbers, the sum of any seven consecutive terms is negative and the sum of any eleven terms is positive. What is the maximum number of terms in the sequence?*

Solution. There can be a maximum of 16 numbers in the sequence. Otherwise, arranging the first 17 numbers in the sequence below:

$$\begin{array}{cccc} a_1 & a_2 & \cdots & a_7 \\ a_2 & a_3 & \cdots & a_8 \\ & & \vdots & \\ a_{11} & a_{12} & \cdots & a_{17} \end{array},$$

by adding the numbers first by rows and then by columns, we get a contradiction. A numerical example for 16 is the following:

$$7, 7, -18, 7, 7, 7, -18, 7, 7, 7, -18, 7, 7, 7, -18, 7.$$

Example 4.43. *Prove the following identities:*

$$1^\circ \quad \sum_{k=0}^{n} k^2 \binom{n}{k}^2 = n(n-1)\binom{2n-2}{n-2} + n\binom{2n-1}{n-1}.$$

$$2^\circ \quad \sum_{k=0}^{n} 2^k \binom{n}{k} \cdot \binom{n-k}{\lfloor \frac{n-k}{2} \rfloor} = \binom{2n+1}{n}.$$

Solution. 1° Clearly, one has

$$\sum_{k=0}^{n} k^2 \binom{n}{k}^2 = \sum_{k=0}^{n} k(k-1)\binom{n}{k}^2 + \sum_{k=0}^{n} k\binom{n}{k}^2,$$

while

$$\sum_{k=0}^{n} k(k-1)\binom{n}{k}^2 = \sum_{k=0}^{n} k(k-1)\binom{n}{k}\binom{n}{n-k}.$$

If A and B are two teams of n players each, then the sum above represents the number of ways in which one can choose n members out of these teams, in such a way that both the leader and deputy are from Team A. For every $k = 0,\ldots,n$, there are $\binom{n}{k}$ ways to choose k players from Team A, $k(k-1)$ ways to designate the leadership, and $\binom{n}{n-k}$ to choose the other $n-k$ players from Team B. If the count is made overall, then there are $n(n-1)$ ways to first choose the leaders from Team A, while the other $n-2$ members can be selected in $\binom{2n-2}{n-2}$ ways. This confirms the relation

$$\sum_{k=0}^{n} k(k-1)\binom{n}{k}^2 = \sum_{k=0}^{n} k(k-1)\binom{n}{k}\binom{n}{n-k} = n(n-1)\binom{2n-2}{n-2}.$$

Similarly, if a single captain has to be selected from Team A, then one obtains

$$\sum_{k=0}^{n} k\binom{n}{k}^2 = \sum_{k=0}^{n} k\binom{n}{k}\binom{n}{n-k} = n\binom{2n-1}{n-1}.$$

2° The right-hand side is the number of ways in which n players can be selected from a team with $2n+1$ players.

We now relate this to the left-hand side. First, divide the players into n groups of 2, with 1 player unpaired. For a given $k = 0,\ldots,n$, there are $\binom{n}{k}$ ways to choose k pairs from where exactly one player is selected, with 2^k such configurations possible, and $\binom{n-k}{\lfloor \frac{n-k}{2} \rfloor}$ ways to select $\lfloor \frac{n-k}{2} \rfloor$ pairs from the $n-k$ pairs from which both players are taken. The unpaired element will not be chosen if $n-k$ is even (as all other elements come in pairs), or it will be chosen if $n-k$ is odd. This ends the proof.

Example 4.44. *Let k and n be positive integers, and consider a set X of n points in the plane with the properties:*

1) no three points in X are collinear
2) for every given point $M \in X$, there are at least k other points in X located at the same distance from M.

Prove that $k < \frac{1}{2} + \sqrt{2n-1}$.

Solution. If $A, B \in X$, then by 1) there can be at most two points $C \in X$ such that $[AC] = [BC]$ (as these are located on the bisector of the segment $[AB]$, and no more than two points in X are collinear). Hence, the number K of triplets (A, B, C) such that $[AC] = [BC]$ satisfies $K \leq 2\binom{n}{2}$. By 2) one also has $K \geq n\binom{k}{2}$, as for each of the n points in X there are at least $\binom{k}{2}$ sets $\{A, B\}$ located at the same distance. Combining these two inequalities one obtains

$$k^2 - k \leq 2(n-1),$$

from where

$$\left(k - \frac{1}{2}\right)^2 = k^2 - k + \frac{1}{4} < k^2 - k + 1 \leq 2n - 1.$$

Taking square roots the desired inequality follows.

Example 4.45. *For a finite set $U \subset \mathbb{N}$, denote by $|U|$, $\sigma(U)$ and $\pi(U)$ the number, the sum and, respectively, the product of the elements in U. If $U = \emptyset$, then $|U| = 0$, $\sigma(U) = 0$ and $\pi(U) = 1$. Prove that*

$$\sum_{U \subseteq S} (-1)^{|U|} \binom{m - \sigma(U)}{|S|} = \pi(S)$$

for all $m \geq \sigma(S)$.

Solution. Say $S = \{x_1, \ldots, x_n\}$. Let R be a set with m elements, containing n pairwise disjoint subsets $A_1, \ldots, A_n$ such that $|A_i| = x_i$. We will count the number of n-element subsets of R meeting each of the A_i 's. Clearly, such a set is obtained by picking one element from each A_i, so there are $x_1 \ldots x_n = \pi(S)$ such sets.

Now, we show that the left hand side counts the same quantity. To see this, let X_i be the set of n-element subsets of R which do not meet A_i. Then $\left|X_{i_1} \cap \ldots \cap X_{i_k}\right| = \binom{m-\sigma(U)}{n}$, where $U = \left\{x_{i_1}, \ldots, x_{i_k}\right\}$. By the Principle of Inclusion and Exclusion, we see that the left hand side counts exactly the number of n-elements subsets of R which meet each of the A_i's.

4.12 Hall's theorem (the marriage theorem)

In this section we present a theoretical result which provides necessary and sufficient conditions for the solubility of the real-life problem below.

Suppose that in a town there are n families $m \geq n$ houses. Each family has preferences over the houses, liking some and disliking others. Establish necessary and sufficient conditions, based on the families' preferences, that would allow for the allocation of a house to each family such that every family receives a house that is to their liking.

Clearly, a necessary condition for the assignment is that every family likes at least one house. However, this condition is not sufficient. Mere fulfillment of this condition does not exclude the possibility that two families like exclusively the same single house. This observation allows us to derive another necessary condition: given any pair of distinct families, the set of houses liked by at least one of them must have at least two elements. Similarly, we deduce that for any set of three families, the set of houses liked by at least one of them must have at least three elements.

Let us denote by F and H the set of families and the set of houses, respectively. We know that $|F| = n$ and $|H| = m$, where $m \geq n$. For every subset $X \subseteq F$, we denote by $H(X) \subseteq H$ the subset of houses liked by at least one family in X. Generalising the previous idea, it is easy to deduce that in order to have a successful allocation of houses, the following necessary condition must hold: for every subset $X \subseteq F$, the cardinality of the set $H(X) \subseteq H$ we must have $|H(X)| \geq |X|$.

The following celebrated theorem of the British mathematician Philip Hall asserts that the condition above is sufficient for the solubility of the problem described above.

Theorem 4.18 (Hall, 1935). *Let F and H be as above. If for every set $X \subseteq F$, we have $|H(X)| \geq |X|$, then there exists an allocation of houses such that each family receives a house that they like.*

Hall's theorem has become commonly known as the **Marriage theorem**, because instead of the families and houses analogy, the theorem is often motivated by asking if it possible to pair two disjoint sets of persons in marriages in a way that all persons from one set are satisfied with their assigned partner?

This problem can be represented using a bipartite graph, where the set of vertices is the disjoint union $F \cup H$. Each edge in the graph represents a possible pairing between a family $f \in F$ and a house $h \in H$. The goal is to find a matching, which is a set of edges that do not share any vertices. In an effort of keeping the book self-contained, we do not use the theory of graphs in our presentation. We recommend the books by Bumbăcea [82] and [252] for detailed accounts of this theorem using graph theory.

Proof. As we remarked above, the condition in the hypothesis is necessary. We prove the sufficiency by strong induction on $|F| = n$. For $n = 1$, the conclusion follows trivially. Assume that the condition is sufficient for $|F| \leq n$ and we will prove that it is also sufficient for $n + 1$. There are two possible cases: either for every subset $X \subseteq F$ we have $|H(X)| \geq |X| + 1$ or, there exists a subset X with $1 \leq |X| = k \leq n$ such that $|H(X)| = |X| = k$.

In the first case, we choose any family $f \in F$ and we pair it with a house $h \in H(\{f\}) \subseteq H$. Now, the remaining sets $F \setminus \{f\}$ and $H \setminus \{h\}$ satisfy the condition of the theorem. We can therefore finish by applying the induction hypothesis.

In the second case, applying the induction hypothesis to X and $H(X)$, we can match the k families with the k houses they like. We are left to prove that we can match the remaining families $F \setminus X$ with the remaining set of houses $H \setminus H(X)$. For any set $Y \subseteq F \setminus X$, from the necessary condition and the fact that Y and X are disjoint, we deduce that $|H(Y \cup X)| \geq |Y| + |X| = |Y| + k$. But since the k families in X like exactly k houses, it follows that $|H(Y)| \geq |Y|$, i.e. the houses in Y like at least $|Y|$ houses. Since Y was chosen arbitrary from $F \setminus X$ and $|F \setminus X| < |X| = n + 1$, we can apply induction hypothesis to $F \setminus X$ to deduce that the remaining families can be paired to the remaining $n + 1 - k$ houses, completing the induction. □

Hall's theorem is a powerful tool and has been applied in many different fields to solve diverse problems. In short, it provides a minimal set of conditions in order to assure a set of preferences can be satisfied in a particular allocation problem. The versatility of Hall's theorem lies in its ability to provide a framework for solving problems that, at first glance, seem unrelated. We illustrate below a list of example problems.

Example 4.46. *An $n \times n$ table is filled with 0's and 1's so that if we chose randomly n cells (no two of them in the same row or column) then at least one of these cells contains 1. Prove that we can find i rows and j columns so that $i + j \geq n + 1$ and their intersection contains only 1's.*

Solution. Let us consider a set of families $F = \{f_1, f_2, \ldots, f_n\}$ and a set of houses $H = \{h_1, h_2, \ldots, h_n\}$ such that the family f_i likes the house h_j if and only if the entry on the position (i, j) in our table is 0.

If for every subset $X \subseteq F$, we have $|H(X)| \geq |X|$, then by Hall's theorem there is an allocation of houses such that each family receives a house they like. In our context, this means that there exists n cells from different rows and columns such that all of them contain 0, a contradiction to the hypothesis. Therefore, the condition in Hall's theorem must not be satisfied.

In other words, there exists a non-empty subset $X \subseteq F$ with the property $|H(X)| < |X|$. Let $k = |X|$ and $l = |H(X)|$. Without losing generality, we may change the ordering of families and houses such that $X = \{f_1, f_2, \ldots, f_k\}$ and also $H(X) = \{h_1, h_2, \ldots, h_l\}$. Looking back to our problem, this means that in the table, the re-labeled lines $1, 2, \ldots k$ and columns $l + 1, \ldots, n$ have only 1's in their intersection.

We have therefore found at least k rows and $n-l$ columns such that

$$k+n-l \geq k+n-k+1 = n+1$$

such that their intersection contains only 1's, which is what we had to prove.

We will now provide an example that can be approached in a manner akin to the one described above.

Example 4.47. *The entries of a $n \times n$ table are non-negative reals such that the numbers in each row and column add up to $s > 0$. Prove that one can pick n numbers from distinct rows and columns which are positive.*

Solution. We first note that by scaling the entries in table, one can assume that $s = 1$. Let us consider a set of families $F = \{f_1, f_2, \ldots, f_n\}$ and a set of houses $H = \{h_1, h_2, \ldots, h_n\}$ such that the family f_i likes the house h_j if and only if the entry on the position (i,j) in our table is different from 0.

If the hypothesis of Hall's theorem holds for F and H, then since there exists a successfully allocation of houses to the n families, each family f_i will correspond to a positive entry (i,j), for different j's, yielding the conclusion.

Let us now prove that the hypothesis of Hall's theorem holds indeed. First let $X \subseteq F$ be any non-empty subset. Remark that the sum of all the numbers on the lines corresponding to families in X is $|X|$. If $H(X) \leq |X| - 1$, there are positive numbers on at most $|X| - 1$ of the intersection of columns with the lines corresponding to families in X, the sum of the numbers on one of these columns would be at least $\frac{|X|}{|X|-1} > 1$, a contradiction with the hypothesis of our problem.

Therefore, for any subset X, we have $|H(X)| \geq |X|$, completing the proof.

Example 4.48. *Some pieces are placed on an 8×8 chessboard. There are exactly 4 pieces in each row and each column of the board. Show that there are 8 pieces among those pieces that no two of them are in the same row or column.*

Solution. Similarly to the first two problems, let us consider a set of families $F = \{f_1, f_2, \ldots, f_8\}$ and a set of houses $H = \{h_1, h_2, \ldots, h_8\}$ such that the family f_i likes the house h_j if and only if there is a piece in the cell (i,j) of the chessboard. We will show that the hypothesis of Hall's theorem is satisfied.

Indeed, for any subset $X \subseteq F$ with $k \geq 2$ elements, we note that these like together $4k$ houses (not necessarily distinct). In other words, $|H(X)| \leq 4k$. If among these $4k$ houses, at most $k-1$ are distinct, then there exists a house which is liked by at least $\frac{4k}{k-1} > 4$ families.

Translated to the setting of our problem, this means that on the column corresponding to this house, there are more than 4 pieces, contradicting the hypothesis. Therefore, for any $X \subseteq F$, we have $|H(X)| \geq |X|$. The conclusion now follows easily.

Example 4.49. *Let X be a finite set and let*

$$X = \bigcup_{i=1}^{n} X_i = \bigcup_{i=1}^{n} Y_i$$

be two disjoint decompositions with all sets X_i and Y_i having the same size. Prove that there are distinct elements $x_1, x_2, \ldots, x_n \in X$ which are in different sets in both decompositions.

Solution. Consider the families $F = \{X_1, X_2, \ldots, X_n\}$ and the houses $H = \{Y_1, Y_2, \ldots, Y_n\}$. We say that the family X_i likes the house Y_j if and only if $X_i \cap Y_j \neq \emptyset$. Note that the conclusion follows if we prove that there is a successful allocation of houses to families.

Now, let $k = |X_i| = |Y_j|$ for all $1 \leq i, j \leq n$. As X_i's are disjoint, the union of any t sets X_i has exactly kt elements. By the same argument, the union of any $t-1$ sets Y_j has exactly $(t-1)k$ elements. As $Y_j's$ cover the whole set X, the tk elements belong to at least t sets Y_j. Looking at Hall's theorem, we just proved that for any $A \subset F$, we have $|H(A)| \geq |A|$. The proof is now complete.

Example 4.50. *Let $P \subset \mathbb{N}$ be a set consisting of* 2005 *distinct prime numbers. Let A be the set of all possible products of* 1002 *elements from P and let B be the set of all products of* 1003 *elements from P. Prove that there is a one-to-one correspondence $f : A \to B$ such that for every $a \in A$, we have that a divides $f(a)$.*

Solution. Consider a set $F = \{f_1, f_2, \ldots, f_n\}$ of $n = \binom{2005}{1002}$ families and a set $H = \{h_1, h_2, \ldots, h_n\}$ of $n = \binom{2005}{1003}$ houses, each of them associated to one of the products with 1002 and 1003 factors, respectively. We say that a family likes a house if the family's number divides the number of the house.

Now, construct a $n \times n$ table in which on the position (i, j) we have $\frac{1}{2003}$ if the family f_i likes the house h_j and 0 otherwise, it is easy to see that on each line and on each column we have non-negative numbers that sum up to 1. From Example 4.47, we deduce that one can pick n numbers from distinct rows and distinct columns which are all positive. That means, there is a successfully allocation of houses to families. This allocation gives the desired one-to-one correspondence f.

Example 4.51. *An $m \times n$ array is filled with the numbers* $1, 2, \ldots, n$ *each used exactly m times. Show that one can always permute the numbers within columns to arrange that each row contains every number* $1, 2, \ldots, n$ *exactly once.*

Solution. We claim that one can permute the numbers within columns to arrange that on the first row we have $\{1, 2, \ldots, n\}$ ordered in some way.

Consider an $n \times n$ table such that in each entry (i, j) we record the number of times i appears on the column j in the original $m \times n$ array.

Note that in this $n \times n$ table, the sum of the numbers on each line is m, since each number appears m times in the initial array. The sum of the numbers on each column is also m, because each column in the initial array contains m entries.

Now, from Example 4.47 we deduce that we can pick n numbers from distinct rows and distinct columns which are all positive. This means that there are n distinct entries in the original $m \times n$ array, lying on different rows and different columns. By permuting elements on each column, these entries can be brought to the first row.

Using the claim, the conclusion follows by an easy induction argument on the number of rows m.

Example 4.52. *A group of students went on a trip to the beach. There were provided n busses of equal capacity for both the trip to the beach and the ride home, one student in each seat. There were not enough seats in $n-1$ buses to fit each student. Every student who left in a bus came back in a bus, but not necessarily the same one. Prove that there are n students such that any two were on different buses on both rides.*

Solution. Let X_i be the set of students in the i-th bus on the trip to the beach and Y_j be the set of the students in the j-th bus on the ride home ($1 \leq i, j \leq n$). Denote by m the number of students that can be seated in a bus. The hypothesis tells us that there are at least $(n-1)m+1$ students in total, as they cannot be seated in $n-1$ busses. We note a striking resemblance to the solution of Example 4.49.

Let $F = \{X_1, \ldots, X_n\}$ be the set of families and $H = \{Y_1, \ldots, Y_n\}$ be the set of houses. We say that the family X_i likes the house Y_j if and only if $X_i \cap Y_j \neq \emptyset$. The problem reduces to showing that there exists a successful allocation of houses to families. Any group of k families contain at least $km - (m-1) = k(m-1)$ students (otherwise a bus can be discarded). Therefore, these students belong to at least k different busses on the ride home. This means that k families like at least k different houses altogether. Now the conclusion follows from Hall's theorem.

Chapter 5
Generating Functions

Generating functions play an important role in the study of sequences of numbers, functions and polynomials (see, e.g., [167, 189, 200, 242, 260]). In this chapter we present key properties, operations and examples involving ordinary generating functions (Section 5.1), or exponential generating functions (Section 5.2). There we give the ordinary and exponential generating functions for some classical polynomials and integer sequences. Section 5.3 contains applications of the Cauchy integral formula in the derivation of integral representations for classical number sequences.

5.1 Ordinary generating functions and examples

The generating function of an infinite sequence

$$a_0, a_1, \ldots, a_n, \ldots,$$

is the infinite series

$$F(z) = a_0 + a_1 z + a_2 z^2 + \cdots + a_n z^n + \cdots. \tag{5.1}$$

The identification principle. Let $F(z) = \sum_{n=0}^{\infty} a_n z^n$ and $G(z) = \sum_{n=0}^{\infty} b_n z^n$ be two generating functions. Then, $F(z) = G(z)$ if and only if $a_n = b_n$, $n \geq 0$.

The following operations hold.

1. Addition.

$$\sum_{n=0}^{\infty} a_n z^n + \sum_{n=0}^{\infty} a_n z^n = \sum_{n=0}^{\infty} c_n z^n, \quad \text{where } c_n = a_n + b_n.$$

2. Multiplication by a constant. If $\alpha \in \mathbb{C}$ a scalar, then

$$\alpha \sum_{n=0}^{\infty} a_n z^n = \sum_{n=0}^{\infty} c_n z^n, \quad \text{where } c_n = \alpha a_n.$$

3. Formal differentiation.

$$\frac{\mathrm{d}}{\mathrm{d}z}\left(F(z)\right)=\frac{\mathrm{d}}{\mathrm{d}z}\left(\sum_{n=0}^{\infty}a_nz^n\right)=\sum_{n=0}^{\infty}na_nz^{n-1}.$$

4. Formal integration.

$$\int F(z)\mathrm{d}z=\int\sum_{n=0}^{\infty}a_nz^n\mathrm{d}z=\sum_{n=0}^{\infty}\frac{a_n}{n+1}z^{n+1}.$$

5. Multiplication.

$$F(z)G(z)=\left(\sum_{n=0}^{\infty}a_nz^n\right)\left(\sum_{n=0}^{\infty}b_nz^n\right)=\sum_{n=0}^{\infty}c_nz^n,$$

where $c_n=\sum_{k=0}^{n}a_kb_{n-k}$.

6. Hadamard multiplication.

$$F(z)\circ G(z)=\left(\sum_{n=0}^{\infty}a_nz^n\right)\left(\sum_{n=0}^{\infty}b_nz^n\right)=\sum_{n=0}^{\infty}c_nz^n,$$

where $c_n=a_nb_n$.

7. Composition. If $a_0=0$, we have

$$G\left(F(z)\right)=\sum_{n=0}^{\infty}b_n\left[F(z)\right]^n=\sum_{n=0}^{\infty}b_n\left(\sum_{\substack{j_1+\cdots+j_k=n\\ j_1,\ldots,j_k\geq 1}}a_{j_1}\cdots a_{j_k}\right)z^n,$$

8. Division. If $b_0\neq 0$, then we have

$$\frac{F(z)}{G(z)}=\frac{\sum_{n=0}^{\infty}a_nz^n}{\sum_{n=0}^{\infty}b_nz^n}=\sum_{n=0}^{\infty}c_nz^n,$$

$$c_n=\frac{1}{b_0}\left(a_n-\sum_{k=1}^{n}b_kc_{n-k}\right).$$

9. Inverse. The power series $F(z)$ and $G(z)$ are inverse if $F(z)G(z)=1$, which implies $a_0b_0=1$ and

$$b_n=-\frac{1}{a_0}\sum_{k=1}^{n}a_kb_{n-k},\quad \text{for } n\geq 1.$$

We now present some illustrative examples of generating functions.

Example 5.1 (Finite sequences). *For example, a finite sequence*

$$a_0, a_1, \ldots, a_n,$$

can be seen as the infinite sequence

$$a_0, a_1, \ldots, a_n, 0, 0, \ldots,$$

whose generating function is the polynomial

$$F(z) = a_0 + a_1 z + a_2 z^2 + \cdots + a_n z^n. \tag{5.2}$$

Example 5.2 (Constant sequence). *The generating function of the sequence*

$$1, 1, \ldots, 1, \ldots$$

is the function

$$F(z) = 1 + z + z^2 + \cdots + z^n + \cdots = \frac{1}{1-z}, \quad |z| < 1.$$

Example 5.3 (Binomial coefficients). *For an integer $n \geq 1$, the generating function for the binomial coefficients*

$$\binom{n}{0}, \binom{n}{1}, \binom{n}{2}, \ldots, \binom{n}{n-1}, \binom{n}{n}, 0, \ldots,$$

is the function

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

Example 5.4 (Generalized binomial coefficients). *Recall that for a real number α and an integer $n \geq 0$, the generalized binomial coefficient is defined by*

$$\binom{\alpha}{n} = \frac{\alpha(\alpha-1)\cdots(\alpha-n+1)}{n!}.$$

The generating function for the generalized binomial coefficients

$$\binom{\alpha}{0}, \binom{\alpha}{1}, \binom{\alpha}{2}, \ldots, \binom{\alpha}{n}, \cdots,$$

is given by

$$\sum_{n=0}^{\infty} \binom{\alpha}{n} z^n = (1+z)^\alpha.$$

Example 5.5. *Let k be a positive integer and let $a_1, a_2, \ldots, a_n, \ldots$, be the infinite sequence whose general term a_n is the number of non-negative integer solutions of the linear Diophantine equation $x_0 + x_1 + \cdots + x_n = n$.*

Solution. The generating function of the sequence $(x_n)_{n\geq 0}$ is

$$\begin{aligned} F(z) &= \sum_{n=0}^{\infty} \left(\sum_{j_1+\cdots+j_k=n} 1 \right) z^n = \sum_{n=0}^{\infty} \sum_{j_1+\cdots+j_k=n} z^{j_1+\cdots+j_k} \\ &= \left(\sum_{j_1=0}^{\infty} z^{j_1} \right) \left(\sum_{j_2=0}^{\infty} z^{j_2} \right) \cdots \left(\sum_{j_k=0}^{\infty} z^{j_k} \right) = \frac{1}{(1-z)^k} \\ &= \sum_{n=0}^{\infty} (-1)^n \binom{-k}{n} z^n = \sum_{n=0}^{\infty} \binom{n+k-1}{n} z^n. \end{aligned}$$

Example 5.6. *Let a_n be the number of integer solutions of the equation*

$$x_1 + x_2 + x_3 = n,$$

where $0 \leq a_1 \leq 4$, $2 \leq a_2 \leq 3$ and $a_3 \geq 3$. Find the generating function.

Solution. The generating function of this sequence is

$$\begin{aligned} F(z) &= \left(1 + z + z^2 + z^3 + z^4\right) \left(z^2 + z^3\right) \left(z^3 + z^4 + \cdots\right) \\ &= \frac{z^5 \left(1 + z + z^2 + z^3 + z^4\right) (1+z)}{1-z}. \end{aligned}$$

Example 5.7. *Find the generating function for the number of n-combinations of red, green, blue and yellow balls, with the properties: the number of red balls is $0, 1, 2$ or 3, the number of green balls is at least 5, the number of blue balls is odd, while the number of yellow balls is even.*

Solution. The generating function of this sequence is

$$\begin{aligned} F(z) &= \left(\sum_{k=0}^{3} z^k \right) \left(\sum_{k=5}^{\infty} z^k \right) \left(\sum_{k=0}^{\infty} z^{2k+1} \right) \left(\sum_{k=0}^{\infty} z^{2k} \right) \\ &= \frac{z^6 \left(1 - z^4\right) \left(1 - z^2\right)^2}{(1-z)^2}. \end{aligned}$$

Example 5.8. *Let k be a positive integer and let $a_0, a_1, \ldots, a_n, \ldots$, be the infinite sequence whose general term a_n is the number of non-negative integer solutions of the linear Diophantine equation*

$$x_1 + x_2 + \cdots + x_k = n.$$

Solution. The generating function of the sequence $(x_n)_{n\geq 0}$ is

$$\begin{aligned} F(z) &= \sum_{n=0}^{\infty} \left(\sum_{j_1+\cdots+j_k=n} 1 \right) z^n = \sum_{n=0}^{\infty} \sum_{j_1+\cdots+j_k=n} z^{j_1+\cdots+j_k} \\ &= \left(\sum_{j_1=0}^{\infty} z_{j_1} \right) \left(\sum_{j_2=0}^{\infty} z_{j_2} \right) \cdots \left(\sum_{j_k=0}^{\infty} z_{j_k} \right) = \frac{1}{(1-z)^k} \\ &= \sum_{n=0}^{\infty} (-1)^n \binom{-k}{n} z^n = \sum_{n=0}^{\infty} \binom{n+k-1}{n} z^n. \end{aligned}$$

Example 5.9. *Let k be a positive integer and let $x_{k,n}$ be the number of integer solutions $(j_1,\ldots,j_k)$ of the equation*

$$a_1 + a_2 + \cdots + a_k = n,$$

such that the numbers $j_1,\ldots,j_k$ are odd positive integers.

The generating function of the sequence $(x_{n,k})_{n\geq 0}$ is

$$\begin{aligned} F(z) &= \left(\sum_{j=0}^{\infty} z^{2j+1} \right) \cdots \left(\sum_{j=0}^{\infty} z^{2j+1} \right) = \frac{z^k}{(1-z^2)^k} \\ &= z^k \sum_{n=0}^{\infty} \binom{n+k-1}{n} z^{2n} = \sum_{n=0}^{\infty} \binom{n+k-1}{n} z^{2n+k}. \end{aligned}$$

Example 5.10. *Find the terms a_n, $n \geq 1$ representing the number of nonnegative integer solutions of the equation*

$$3x_1 + 4x_2 + x_3 + 5x_4 = n.$$

Solution. The generating function of the sequence $(a_n)_{n\geq 0}$ is

$$\begin{aligned} F(z) &= \left(\sum_{k=0}^{\infty} z^{3k} \right) \left(\sum_{k=0}^{\infty} z^{4k} \right) \left(\sum_{k=0}^{\infty} z^{k} \right) \left(\sum_{k=0}^{\infty} z^{5k} \right) \\ &= \frac{1}{(1-z^3)(1-z^4)(1-z)(1-z^5)}. \end{aligned}$$

More generally, if for an integer $k \geq 1$ and given integers $a_1,\ldots,a_k$, then the number of integer solutions $(x_1,\ldots,x_k)$ of the equation

$$a_1x_1 + a_2x_2 + \cdots + a_kx_k = n,$$

is given by the formula

$$F(z) = \frac{1}{(1-z^{a_1})(1-z^{a_2})\cdots(1-z^{a_k})}.$$

Note that we also have the following useful identities:

$$\frac{1}{(1-z)^n} = \sum_{k=0}^{\infty} \binom{-n}{k} (-z)^k = \sum_{k=0}^{\infty} \binom{n+k-1}{k} z^k, \quad |z| < 1;$$
$$\frac{1}{(1-az)^n} = \sum_{k=0}^{\infty} \binom{-n}{k} (-az)^k = \sum_{k=0}^{\infty} \binom{n+k-1}{k} a^k z^k, \quad |z| < \frac{1}{|a|}.$$

These formulae help to find the generating functions for many sequences.

Example 5.11. *Show that the generating function of the sequence*

$$0, 1, 2^2, \ldots, n^2, \ldots,$$

is given by the formula

$$F(z) = \frac{z(1+z)}{(1-z)^3}.$$

Solution. Indeed, we have $\dfrac{1}{1-z} = \sum\limits_{k=0}^{\infty} z^k$, hence

$$\frac{1}{(1-z)^2} = \frac{\mathrm{d}}{\mathrm{d}z}\left(\frac{1}{1-z}\right) \sum_{k=0}^{\infty} \frac{\mathrm{d}}{\mathrm{d}z}\left(z^k\right)$$
$$= \sum_{k=0}^{\infty} k z^{k-1}.$$

Multiplying both sides by z we obtain $\dfrac{z}{(1-z)^2} = \sum\limits_{k=0}^{\infty} k z^k$, which by differentiation with respect to z gives

$$\frac{1+z}{(1-z)^3} = \sum_{k=0}^{\infty} k^2 z^{k-1}.$$

The desired result is obtained by multiplication with z.

Similarly one can obtain the generating functions for the sequence

$$0, 1, 2^k, \ldots, n^k, \ldots,$$

where $k \geq 2$ is a fixed integer.

The sequence $(C_n)_{n\geq 0}$ given by

$$C_n = \frac{1}{n+1}\binom{2n}{n},$$

is known as the Catalan sequence, which has numerous interpretations and practical applications.

Example 5.12 (Catalan sequence). *Consider the Catalan sequence given by*

$$C_{n+1} = \sum_{k=0}^{n} C_k C_{n-k}, \quad C_0 = 1.$$

Prove that $C_n = \dfrac{1}{n+1}\binom{2n}{n}$.

Solution. Using the generating function $F(z) = \sum_{n=0}^{\infty} C_n z^n$, we have

$$\begin{aligned} F(z)F(z) &= \left(\sum_{n=0}^{\infty} C_n z^n\right)\left(\sum_{n=0}^{\infty} C_n z^n\right) = \sum_{n=0}^{\infty}\left(\sum_{k=0}^{\infty} C_k C_{n-k}\right) z^n \\ &= \sum_{n=0}^{\infty} C_{n+1} z^n = \frac{1}{z}\sum_{n=1}^{\infty} C_n z^n = \frac{F(z)}{z} - \frac{1}{z}, \end{aligned}$$

hence the following identity holds $zF(z)^2 - F(z) + 1 = 0$.

Solving for $F(z)$ we obtain

$$F(z) = \frac{1 \pm \sqrt{1-4z}}{2z}.$$

Since we have

$$\sqrt{1-4z} = 1 + \sum_{n=1}^{\infty} (-1)^n \binom{\frac{1}{2}}{n} 4^n z^n = 1 + \sum_{n=1}^{\infty} a_n z^n,$$

with

$$\begin{aligned} a_n &= (-1)^n \left[\frac{1}{2}\left(\frac{1}{2}-1\right)\cdots\left(\frac{1}{2}-n+1\right)\right]\cdot\frac{2^n}{n!}\cdot 2^n \\ &= (-1)^n \frac{(-1)(-3)\cdots(-2(n-1)+1)}{n!}\cdot 2^n \\ &= -\frac{1\cdot 3\cdot 5\cdots(2(n-1)-1)}{n!}\cdot 2^n = -2\frac{(2(n-1))!}{n!(n-1)!}. \end{aligned}$$

It follows that

$$\sqrt{1-4z} = 1 - 2\sum_{n=0}^{\infty} \frac{(2n)!}{n!(n+1)!} z^{n+1},$$

hence

$$F(z) = \frac{1-\sqrt{1-4z}}{2z} = \sum_{n=0}^{\infty} \frac{(2n)!}{n!(n-1)!} z^n = \sum_{n=0}^{\infty} \frac{1}{n+1}\binom{2n}{n} z^n.$$

Remark. One can prove by induction that C_n is the number of ways to add brackets to evaluate the matrix product

$$A_1 A_2 \cdots A_{n+1}, \quad n \geq 0.$$

The number of ways to evaluate the product $A_1 A_2 \cdots A_{n+1}$ is determined by multiplying two matrices at the end, which is given exactly by $n+1$, i.e.,

$$A_1 A_2 \cdots A_{n+1} = (A_1 \cdots A_k)(A_{k+1} \cdots A_{n+1}), \quad 0 \leq k \leq n.$$

This suggests that the following recurrence relation holds:

$$C_{n+1} = \sum_{k=0}^{n} C_k C_{n-k},$$

which produces Catalan's sequence.

5.2 Exponential generating functions and examples

The method of ordinary generating functions helped finding sequence terms, especially when these were linked to binomial coefficients. However, in other applications, generating functions with different properties must be considered. Such examples are the exponential generating functions.

For the sequence $(a_n)_{n\geq 0}$, the exponential generating function is the series

$$E(z) = \sum_{n=0}^{\infty} \frac{a_n}{n!} z^n. \tag{5.3}$$

The identification principle. If $F(z) = \sum_{n=0}^{\infty} \frac{1}{n!} a_n z^n$ and $G(z) = \sum_{n=0}^{\infty} \frac{1}{n!} b_n z^n$ are two generating functions, then $F(z) = G(z)$ if and only if $a_n = b_n$, $n \geq 0$.

The following operations are defined.

1. Addition.

$$\sum_{n=0}^{\infty} \frac{1}{n!} a_n z^n + \sum_{n=0}^{\infty} \frac{1}{n!} a_n z^n = \sum_{n=0}^{\infty} \frac{1}{n!} c_n z^n, \quad \text{where } c_n = a_n + b_n.$$

2. Multiplication by a constant. If $\alpha \in \mathbb{C}$ a scalar, then

$$\alpha \sum_{n=0}^{\infty} \frac{1}{n!} a_n z^n = \sum_{n=0}^{\infty} \frac{1}{n!} c_n z^n, \quad \text{where } c_n = \alpha a_n.$$

3. Formal differentiation.

$$\frac{\mathrm{d}}{\mathrm{d}z}\left(F(z)\right)=\frac{\mathrm{d}}{\mathrm{d}z}\left(\sum_{n=0}^{\infty}\frac{1}{n!}a_nz^n\right)=\sum_{n=0}^{\infty}\frac{1}{n!}na_nz^{n-1}=\sum_{n=0}^{\infty}\frac{1}{n!}a_{n+1}z^n.$$

4. Formal integration.

$$\int F(z)\mathrm{d}z=\int\sum_{n=0}^{\infty}\frac{1}{n!}a_nz^n\mathrm{d}z=\sum_{n=0}^{\infty}\frac{1}{n!}\frac{a_n}{n+1}z^{n+1}=\sum_{n=1}^{\infty}\frac{1}{n!}a_{n-1}z^n.$$

4. Multiplication.

$$F(z)G(z)=\left(\sum_{n=0}^{\infty}\frac{1}{n!}a_nz^n\right)\left(\sum_{n=0}^{\infty}\frac{1}{n!}b_nz^n\right)=\sum_{n=0}^{\infty}\frac{1}{n!}c_nz^n,$$
$$c_n=\sum_{k=0}^{n}\binom{n}{k}a_kb_{n-k}.$$

5. Hadamard multiplication.

$$F(z)\circ G(z)=\left(\sum_{n=0}^{\infty}\frac{1}{n!}a_nz^n\right)\left(\sum_{n=0}^{\infty}\frac{1}{n!}b_nz^n\right)=\sum_{n=0}^{\infty}\frac{1}{n!}c_nz^n,$$

where $c_n=\dfrac{1}{n!}a_nb_n$.

6. Composition. If $a_0=0$, we have

$$\begin{aligned}G\left(F(z)\right)&=\sum_{n=0}^{\infty}\frac{1}{n!}b_n\left[F(z)\right]^n\\&=\sum_{n=0}^{\infty}\frac{1}{n!}b_n\left(\sum_{\substack{j_1+\cdots+j_k=n\\j_1,\ldots,j_k\geq1}}\frac{a_{j_1}}{j_1!}\cdots\frac{a_{j_k}}{j_k!}\right)z^n\\&=\sum_{n=0}^{\infty}\frac{1}{n!}b_n\left(\sum_{\substack{j_1+\cdots+j_k=n\\j_1,\ldots,j_k\geq1}}\frac{1}{n!}\binom{n}{j_1,\ldots,j_k}a_{j_1}\cdots a_{j_k}\right)z^n.\end{aligned}$$

7. Division. If $b_0\neq0$, then we have

$$\frac{F(z)}{G(z)}=\frac{\sum_{n=0}^{\infty}\frac{1}{n!}a_nz^n}{\sum_{n=0}^{\infty}\frac{1}{n!}b_nz^n}=\sum_{n=0}^{\infty}\frac{1}{n!}c_nz^n,\text{ where}$$
$$c_n=\frac{1}{b_0}\left(a_n-\sum_{k=1}^{n}\binom{n}{k}b_kc_{n-k}\right).$$

8. Inverse. The power series $F(z)$ and $G(z)$ are inverse if $a_0 b_0 = 1$ and

$$b_n = -\frac{1}{a_0} \sum_{k=1}^{n} \binom{n}{k} a_k b_{n-k}, \quad \text{for } n \geq 1.$$

The following exponential generating functions are immediate

- $a_n = 1$, $n \geq 0$ (constant sequence)

$$E(z) = \sum_{k=0}^{\infty} \frac{z^k}{k!} = e^z.$$

- $a_n = a^n$, $n \geq 0$ and $a \in \mathbb{C}$ a complex number (geometric sequence)

$$E(z) = \sum_{k=0}^{\infty} \frac{a^k z^k}{k!} = \sum_{k=0}^{\infty} \frac{(az)^k}{k!} = e^{az}.$$

- If $0 \leq k \leq n$ be positive integers and $P(n,k) = \frac{n!}{(n-k)!}$ is the number of arrangements of k objects out of n, then the exponential generating function of the sequence $P(n,0), P(n,1), P(n,2), \ldots, P(n,n), 0, \ldots$, is given by

$$E(z) = \sum_{k=0}^{n} \frac{P(n,k)}{k!} z^k = \sum_{k=0}^{n} \binom{n}{k} z^k = (1+z)^k.$$

Theorem 5.1 (n-permutations of multisets). *Let $M = \{n_1\alpha_1, n_2\alpha_2, \ldots, n_k\alpha_k\}$ be a multiset over the set $S = \{\alpha_1, \alpha_2, \ldots, \alpha_k\}$, where n_j is multiplicity of the element α_j, $j = 1, \ldots, k$. Denoting by a_n the number of n-permutations of the multiset M, the exponential generating function of the sequence $(a_n)_{n\geq 0}$ is*

$$E(z) = \left(\sum_{j=0}^{n_1} \frac{z^j}{j!}\right)\left(\sum_{j=0}^{n_2} \frac{z^j}{j!}\right) \cdots \left(\sum_{j=0}^{n_k} \frac{z^j}{j!}\right). \tag{5.4}$$

Proof. Notice that for $n \geq n_1 + \cdots + n_k$, we have $a_n = 0$, hence $E(z)$ is a polynomial. Notice also that the right side of (5.4) can be expanded as

$$\sum_{j_1, j_2, \ldots, j_k = 0}^{n_1, n_2, \ldots, n_k} \frac{z^{j_1 + j_2 \cdots + j_k}}{j_1! j_2! \cdots j_k!} = \sum_{n=0}^{n_1 + n_2 + \cdots + n_k} \frac{z^n}{n!} \sum_{\substack{j_1 + \cdots + j_k \\ 0 \leq j_1 \leq n_1, \ldots, 0 \leq j_k \leq n_k}} \frac{n!}{j_1! j_2! \cdots j_k!}$$

The number of permutations of M with exactly $j_1\alpha_1's$, $j_2\alpha_2's$, $\ldots$, $j_k\alpha_k's$ such that $j_1 + j_2 + \cdots + j_k = n$ is the multinomial coefficient

$$\binom{n}{j_1, j_2, \ldots, j_k} = \frac{n!}{j_1! j_2! \cdots j_k!}.$$

This shows that a_n is indeed given by $a_n = \sum_{\substack{j_1+\cdots+j_k \\ 0\le j_1\le n_1,\ldots,0\le j_k\le n_k}} \frac{n!}{j_1!j_2!\cdots j_k!}$. □

Example 5.13. *Determine the number of ways to colour the squares of a* 1*-by-n chessboard using black, white, green and red, if an even number of squares if coloured in black.*

Solution. Denoting the numbers of colourings by a_n, we have $a_1 = 0$. Each such colouring can be seen as a permutation of three objects b (black), w (white), g (green) and r (red), with repetitions allowed, where b appears an even number of times. This is given by the exponential generating function expressed by the formula

$$\begin{aligned} E(z) &= \left(\sum_{n=0}^{\infty} \frac{z^{2n}}{(2n)!}\right)\left(\sum_{n=0}^{\infty} \frac{z^n}{n!}\right)^3 \\ &= \frac{e^z + e^{-z}}{2} e^{3z} = \frac{1}{2}\left(e^{4z} + e^{2z}\right) \\ &= \frac{1}{2}\left(\sum_{n=0}^{\infty} \frac{4^n z^n}{n!} + \sum_{n=0}^{\infty} \frac{2^n z^n}{n!}\right) = \frac{1}{2}\sum_{n=0}^{\infty} (4^n + 2^n)\cdot \frac{z^n}{n!}. \end{aligned}$$

This shows that $a_n = 2^{n-1}(2^n + 1)$, $n \ge 1$.

Example 5.14. *Determine the number a_n of n digit (in base* 10*) numbers with each digit even, where the digits* 0, 2 *and* 4 *occur an even number of times.*

Solution. Denoting this number by a_n and setting $a_1 = 0$, this is the number of n-permutations of the multiset $M = \{\infty 0, \infty 2, \infty 4, \infty 6, \infty 8\}$ (having infinitely many copies of each element), in which 0, 2 and 4 occur an even number of times. The exponential generating function is

$$\begin{aligned} E(z) &= \left(\sum_{n=0}^{\infty} \frac{z^{2n}}{(2n)!}\right)^3 \left(\sum_{n=0}^{\infty} \frac{z^n}{n!}\right)^2 = \left(\frac{e^z + e^{-z}}{2}\right)^3 e^{2z} \\ &= \frac{1}{8}\left(e^{-z} + 3e^z + 3e^{3z} + e^{5z}\right) \\ &= \frac{1}{8}\left(\sum_{n=0}^{\infty} \frac{(-1)^n z^n}{n!} + 3\sum_{n=0}^{\infty} \frac{z^n}{n!} + 3\sum_{n=0}^{\infty} \frac{3^n z^n}{n!} + \sum_{n=0}^{\infty} \frac{5^n z^n}{n!}\right) \\ &= \frac{1}{8}\sum_{n=0}^{\infty} (5^n + 3^n + 1 + (-1)^n)\cdot \frac{z^n}{n!}. \end{aligned}$$

This shows that

$$a_n = \frac{5^n + 3^n + 1 + (-1)^n}{8}, \quad n \ge 0.$$

Example 5.15. *Find the number of ways to colour the squares of a* 1*-by-n board with red, blue, green and white, where the number of red squares is odd, the number of blue squares is even, and at least one square is white.*

Solution. The exponential generating function is

$$\begin{aligned} E(z) &= \left(\sum_{n=0}^{\infty} \frac{z^{2n+1}}{(2n+1)!}\right)\left(\sum_{n=0}^{\infty} \frac{z^{2n}}{(2n)!}\right)\left(\sum_{n=0}^{\infty} \frac{z^n}{n!}\right)\left(\sum_{n=1}^{\infty} \frac{z^n}{n!}\right) \\ &= \left(\frac{e^z - e^{-z}}{2}\right)\left(\frac{e^z + e^{-z}}{2}\right) e^z(e^z - 1) \\ &= \frac{1}{4}\left(e^{4z} - e^{3z} - 1 + e^{-z}\right) \\ &= -\frac{1}{4} + \frac{1}{4}\sum_{n=0}^{\infty} (4^n - 3^n + (-1)^n) \cdot \frac{z^n}{n!}. \end{aligned}$$

This shows that

$$a_n = \frac{4^n - 3^n + (-1)^n}{4}, \quad n \geq 1,$$

and $a_0 = 0$.

5.3 A useful version of the Cauchy integral formula

The Cauchy integral formula is a fundamental result in complex analysis, with a long history and applications in areas like complex analysis, combinatorics, discrete mathematics, or number theory.

Here we will use a version of Cauchy's formula derived in [16], to derive integral representations for the terms of some classical integer sequences. Recently, this approach was used to compute exact integral formulae for the coefficients of cyclotomic [20], Gaussian and multinomial [17], polygonal [18], and other general classes of polynomials [19].

Recall that a function $h : \Omega \to \mathbb{C}$ is said to be *meromorphic* at a point $z_0 \in \Omega$, if h can be written as a quotient of two analytic functions f, g in a neighbourhood $\mathcal{U} \subset \Omega$ of z_0

$$\forall z \in \mathcal{U} \setminus \{z_0\} \; : \; h(z) = \frac{f(z)}{g(z)}.$$

In this case we also have the expansion

$$h(z) = \sum_{n \geq -m} c_n (z - z_0)^n, \tag{5.5}$$

for all $z \neq z_0$ in a disk centered at z_0. If m is the largest number for which $c_{-m} \neq 0$ in (5.5), then z_0 is called a *pole* of order m. The coefficient c_{-1} in the

expression $(z-z_0)^{-1}$ in (5.5) is denoted by $\mathrm{Res}(h,z_0)$, and called the *residue* of h at the point z_0. Cauchy's Residue theorem relates global properties of a meromorphic function and its integral along closed curves, to local characteristics, i.e., the residues at poles.

Theorem 5.2 (Residue theorem). *Let $h:\Omega\to\mathbb{C}$ be a meromorphic function in a domain Ω, and λ be a simple loop in Ω along which the function is analytic. Then*

$$\frac{1}{2\pi i}\int_\lambda h(z)\,\mathrm{d}z=\sum_s Res(h(z),z=s),$$

where the sum is over all poles s of h enclosed by λ.

Through this formula one can obtain a unitary formula for the coefficients of an analytic function [124].

Theorem 5.3 (Cauchy integral formula). *Let $f(z)=\sum_{n\geq 0}c_n z^n$ be an analytic function in a disk centered at 0, and let Γ be a curve in the interior of this disk, which winds around the origin exactly once in positive orientation, that is the winding number with respect to 0 is equal to 1. Then we have*

$$c_n=\frac{1}{2\pi i}\int_\Gamma \frac{f(z)}{z^{n+1}}\,\mathrm{d}z,\quad n=0,1,\ldots. \tag{5.6}$$

Letting Γ be the circle of radius $R>0$ centred at 0 and $z=R(\cos t+i\sin t)$, with $t\in[0,2\pi]$, we have $\mathrm{d}z=R(-\sin t+i\cos t)\mathrm{d}t=iR(\cos t+i\sin t)\mathrm{d}t$. Then, formula (5.6) can be written as

$$\begin{aligned}c_n&=\frac{1}{2\pi i}\int_0^{2\pi}\frac{iR(\cos t+i\sin t)f\left(R(\cos t+i\sin t)\right)}{R^{n+1}(\cos t+i\sin t)^{n+1}}\,\mathrm{d}t\\&=\frac{1}{2\pi R^n}\int_0^{2\pi}\frac{f\left(R(\cos t+i\sin t)\right)}{\cos nt+i\sin nt}\,\mathrm{d}t,\end{aligned}$$

therefore

$$c_n=\frac{1}{2\pi R^n}\int_0^{2\pi}(\cos nt-i\sin nt)f\left(R(\cos t+i\sin t)\right)\,\mathrm{d}t,\quad n=0,1,\ldots. \tag{5.7}$$

If the coefficients c_n are real numbers, then from (5.7), for $n=0,1,\ldots$ we obtain

$$c_n=\frac{1}{2\pi R^n}\int_0^{2\pi}\mathrm{Re}\left[(\cos nt-i\sin nt)f\left(R(\cos t+i\sin t)\right)\right]\,\mathrm{d}t. \tag{5.8}$$

In addition, in this case the following formula can be deduced

$$\int_0^{2\pi}\mathrm{Im}\left[(\cos nt-i\sin nt)f\left(R(\cos t+i\sin t)\right)\right]\,\mathrm{d}t=0,\quad n=0,1,\ldots.$$

Remark. When f is a polynomial, we can give a direct proof to formula (5.7). Indeed, assuming that $f(z) = \sum_{k=0}^{m} c_k z^k$, we obtain

$$z^{-n} f(z) = c_n + \sum_{k=0, k\neq n}^{m} c_k z^{k-n}.$$

Let $z = R(\cos t + i \sin t)$, $t \in [0, 2\pi]$, and consider the integral over the interval $[0, 2\pi]$. Clearly, the integral of z^{k-n} vanishes for $k \neq n$, hence

$$\int_0^{2\pi} R(\cos t + i \sin t)^{-n} f\left(R(\cos t + i \sin t)\right) \mathrm{d}t = 2\pi c_n, \quad n = 0, 1, \ldots, \quad (5.9)$$

so (5.7) follows. The above argument also works for Laurent polynomials.

Example 5.16. *Let with $0 < R < 1$ and consider the geometric series $\sum_{n\geq 0} z^n$. Clearly, we have $f(z) = \frac{1}{1-z}$ and*

$$f\left(R(\cos t + i \sin t)\right) = \frac{1}{1 - R(\cos t + i \sin t)} = \frac{1 - R(\cos t - i \sin t)}{1 + R^2 - 2R \cos t}.$$

By formula (5.7) *it follows that for every $n \geq 0$, we have*

$$\begin{aligned} 1 = c_n &= \frac{1}{2\pi R^n} \int_0^{2\pi} \frac{(\cos nt - i \sin nt)\left[1 - R(\cos t - i \sin t)\right]}{1 + R^2 - 2R \cos t} \mathrm{d}t \\ &= \frac{1}{2\pi R^n} \int_0^{2\pi} \frac{\cos nt - R \cos(n+1)t - i\left[\sin nt - R \sin(n+1)t\right]}{1 + R^2 - 2R \cos t} \mathrm{d}t. \end{aligned}$$

Because the coefficients c_n are real numbers, from (5.8) *we obtain*

$$1 = \frac{1}{2\pi R^n} \int_0^{2\pi} \frac{\cos nt - R \cos(n+1)t}{1 + R^2 - 2R \cos t} \mathrm{d}t,$$

and

$$0 = \frac{1}{2\pi R^n} \int_0^{2\pi} \frac{\sin nt - R \sin(n+1)t}{1 + R^2 - 2R \cos t} \mathrm{d}t.$$

Chapter 6
Recursive Processes

Many mathematical patterns can be described using the idea of recursion. Recursion is a process in which each step of a pattern is dependent on the step or steps that come before it. In this chapter we will present recursive processes of first order, second order, and also higher-order.

In this process we will also investigate the Fibonacci numbers and related sequences, for which we give exact formulae for the general terms, as well as various properties, formulae and interpretations.

We begin with an illustrative example.
Recall the number D_n of **derangements** of a set with n elements is

$$D_n = n!\left(1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \cdots (-1)^n \frac{1}{n!}\right).$$

This formula is not useful if we want to compute D_n for some concrete values of n. Two formulas connecting D_n with D_{n-1}, or with D_{n-1} and D_{n-2}, are given in the following examples.

Example 6.1 (The first recursive formula for D_n). *The following formula holds:*

$$D_{n+1} = (n+1)D_n + (-1)^{n+1}, \quad n = 1,2,3,\ldots.$$

Solution. Just write

$$\begin{aligned} nD_{n-1} + (-1)^n &= nD_{n-1} + n!\frac{(-1)^n}{n!} \\ &= n!\left(1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \cdots + (-1)^{n-1}\frac{1}{(n-1)!}\right) + n!\frac{(-1)^n}{n!} \\ &= n!\left((1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \cdots + (-1)^n \frac{1}{n!}\right) = D_n. \end{aligned}$$

Finally, replace n by $n+1$.

Example 6.2 (Another recursive formula for D_n). *The following formula holds:*

$$D_{n+2} = (n+1)(D_{n+1} + D_n), \quad n = 1,2,3,\ldots$$

Solution. Using twice the first recursion formula, we have

$$\begin{aligned}(n+1)(D_{n+1} + D_n) &= (n+1)D_{n+1} + (n+1)D_n \\ &= (n+1)D_{n+1} + D_{n+1} - (-1)^{n+1} \\ &= (n+2)D_{n+1} + (-1)^{n+2} = D_{n+2}.\end{aligned}$$

Let $k \geq 1$ be a fixed integer, and let $(f_n)_{n\geq 0}$ be a sequence of functions in k variables. A **recursive sequence** defined by $(f_n)_{n\geq 1}$ is a sequence $(a_n)_{n\geq 0}$ of numbers satisfying

$$a_{n+k} = f_{n+k}(a_{n+k-1}, a_{n+k-2}, \ldots, a_n)$$

for any $n \geq 0$, i.e., the $(n+k)^{th}$ entry of the sequence is uniquely determined by the k entries before it. The above relation is called a **recursive relation of order** k. If the first k terms of the sequence $(a_n)_{n\geq 0}$ are given, then the sequence is perfectly determined by the recursive relation.

Properties of the sequence of functions $(f_n)_{n\geq 0}$ will define various classes of recursive relations. In Example 6.1, the sequence of functions $(f_n)_{n\geq 0}$, is defined by the formula $f_{n+1}(x) = (n+1)x + (-1)^{n+1}$, $n = 1,2,\ldots$; Then, in Example 6.2, the sequence of functions $(f_n)_{n\geq 1}$, is defined by the formula $f_{n+2}(x) = (n+1)(x+y)$, $n = 1,2,\ldots$.

6.1 First order recursions

Let α, a, b be given real numbers. In many situations one must find the formula for x_n, where $(x_n)_{n\geq 0}$ is a sequence defined by $x_0 = \alpha$ and

$$x_{n+1} = ax_n + b, \quad n = 0,1,2,\ldots. \tag{6.1}$$

The sequence of functions $(f_n)_{n\geq 0}$ is defined $f_n(x) = ax + b, n = 0,1,\ldots$

The following special cases are clear.

- If $a = 1$, $b \neq 0$, then $(x_n)_{n\geq 0}$ is an arithmetic sequence and

$$x_n = \alpha + nb.$$

- If $a = 0$, then $(x_n)_{n\geq 0}$ is the constant sequence $x_n = b$, $n = 1,2,\ldots$.
- If $a = 1$, $b = 0$, then $(x_n)_{n\geq 0}$ is a geometric sequence and

$$x_n = a\alpha^{n-1}, \quad n = 1,2,\ldots.$$

In the generic case $a \neq 1$, $a \neq 0$ and $b \neq 0$ we proceed as follows. In the first step we find a real number x such that $x_{n+1} + x = a(x_n + x)$, $n = 0,1,\ldots$.

For $n = 0$, we get $x_1 + x = a(x_0 + x)$ and $x_1 = ax_0 + b$, hence $x = \frac{b}{a-1}$. For the second step, introduce the sequence $(y_n)_{n\geq 0}$, $y_n = x_n + x$. We obtain $y_{n+1} = ay_n$, $n = 0,1,\ldots$, hence $(y_n)_{n\geq 0}$ is a geometric sequence.

It follows that $y_n = a^n y_0$, $n = 0,1,2,\ldots$, so

$$x_n = a^n \left(\alpha + \frac{b}{a-1}\right) - \frac{b}{a-1}, \quad n = 0,1,2,\ldots. \tag{6.2}$$

Example 6.3. *Consider the sequence $(x_n)_{n\geq 0}$ defined by $x_0 = 0$ and $x_{n+1} = -\frac{1}{2}x_n + 1$, $n = 0,1,2,\ldots$. Find a formula for x_n.*

Solution. Applying formula (6.2) for $\alpha = 0$, $a = -\frac{1}{2}$, $b = 1$, we obtain

$$\begin{aligned} x_n &= \left(-\frac{1}{2}\right)^n \left(\frac{1}{-\frac{1}{2}-1}\right) + \frac{1}{\frac{1}{2}+1} \\ &= \left(-\frac{1}{2}\right)^n \left(-\frac{2}{3}\right) + \frac{2}{3} \\ &= \frac{(-1)^{n+1}}{3\cdot 2^{n-1}} + \frac{2}{3}, \quad n = 0,1,2,\ldots. \end{aligned}$$

Example 6.4. *Let $(x_n)_{n\geq 0}$ be the sequence defined by $x_0 = \alpha$ and $x_{n+1} = x_n + n$, $n = 0,1,2,\ldots$. Find x_{2025}.*

Solution. Note that in this case the recursion defining the sequence $(x_n)_{n\geq 0}$ is not of type (6.1), hence we cannot apply the method above to find x_n. In this case we write the recursion relation for $n = 0,1,2,\ldots$, and get

$$\begin{aligned} &x_1 - x_0 = 0 \\ &x_2 - x_1 = 1 \\ &x_3 - x_2 = 2 \\ &\cdots\cdots\cdots \\ &x_n - x_{n-1} = n-1. \end{aligned}$$

Summing up all these relations we obtain

$$x_n - x_0 = 1 + 2 + \cdots + n - 1 = \frac{(n-1)n}{2}.$$

Therefore, $x_n = \alpha + \frac{(n-1)n}{2}$ and

$$x_{2025} = \alpha + \frac{2024\cdot 2025}{2}.$$

6.2 Second order linear recursions

Let $(x_n)_{n\geq 0}$ be the sequence defined by $x_0 = \alpha_0$, $x_1 = \alpha_1$, and

$$x_{n+2} = ax_{n+1} + bx_n, \quad n = 0,1,2,\ldots, \tag{6.3}$$

where α_0, α_1, a, b are given real numbers.

One can define the sequence of functions $(f_n)_{n\geq 0}$ given by the formula $f_n(x,y) = ax + by$, $n = 0,1,\ldots$, where we have $k = 2$ and all the functions in the sequence are linear. These properties motivate the name of the recursion.

In the search for solutions of the equation (6.3), one may try expressions of the form $x_n = t^n$. By substitution in the original equation

$$t^n \left(t^2 - at - b\right) = 0.$$

A trivial solution is obtained for $t = 0$, so we shall assume for now that $t \neq 0$. The **characteristic equation** of sequence $(x_n)_{n\geq 0}$, is defined by

$$t^2 - at - b = 0. \tag{6.4}$$

Depending on whether the two roots t_1, t_2 of the characteristic equation (6.4) are distinct or equal, one may identify two cases.

Case 1. Distinct roots. If the roots t_1, t_2 of (6.4) are distinct (real or complex), then the sequences $(t_1^n)_{n\geq 0}$ and $(t_2^n)_{n\geq 0}$ are both solutions of (6.3).

The general formula is given by the linear combination

$$x_n = c_1 t_1^n + c_2 t_2^n, \quad n = 0,1,2,\ldots, \tag{6.5}$$

where coefficients c_1 and c_2 are determined by the system of linear equations

$$\begin{cases} c_1 + c_2 = \alpha_0 \\ c_1 t_1 + c_2 t_2 = \alpha_1. \end{cases} \tag{6.6}$$

Case 2. Equal roots. If $t_1 = t_2$, then the solution of (6.3) is given by

$$x_n = (c_1 + c_2 n)\, t_1^n, \quad n = 0,1,2,\ldots, \tag{6.7}$$

where coefficients c_1 and c_2 are determined by the system

$$\begin{cases} c_1 = \alpha_0 \\ (c_1 + c_2)\, t_2 = \alpha_1. \end{cases}$$

The relations (6.5) and (6.7) are often called **Binet-type formulae**. Initially formulated by Binet in 1843 in the context of the Fibonacci sequence, numerous Binet-type formulae exist for similar sequences, including the case of recurrent sequences of higher order.

We now present a matrix formula which allows the calculation of the terms of the sequence $(x_n)_{n\geq 0}$ given by (6.3). We start with two identities.

Remark. For a,b,c,d real numbers, the following identity holds

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} d & c \\ b & a \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^{-1} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}. \tag{6.8}$$

Theorem 6.1. *The following formulae hold*

$$1^\circ \quad \begin{pmatrix} x_{n-1} & x_n \\ x_n & x_{n+1} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ b & a \end{pmatrix}^{n-1} \begin{pmatrix} x_0 & x_1 \\ x_1 & x_2 \end{pmatrix}. \tag{6.9}$$

$$2^\circ \quad \begin{pmatrix} x_{n+1} & x_n \\ x_n & x_{n-1} \end{pmatrix} = \begin{pmatrix} a & b \\ 1 & 0 \end{pmatrix}^{n-1} \begin{pmatrix} x_2 & x_1 \\ x_1 & x_0 \end{pmatrix}, \tag{6.10}$$

where $n = 1,2,\ldots$.

Proof. 1° Note that the following matrix relation holds for $n \geq 2$

$$\begin{pmatrix} x_{n-1} & x_n \\ x_n & x_{n+1} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ b & a \end{pmatrix} \begin{pmatrix} x_{n-2} & x_{n-1} \\ x_{n-1} & x_n \end{pmatrix},$$

hence, we can write

$$\begin{pmatrix} x_{n-1} & x_n \\ x_n & x_{n+1} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ b & a \end{pmatrix}^{n-1} \begin{pmatrix} x_0 & x_1 \\ x_1 & x_2 \end{pmatrix}.$$

2° By the remark we obtain

$$\begin{pmatrix} 0 & 1 \\ b & a \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^{-1},$$

$$\begin{pmatrix} 0 & 1 \\ b & a \end{pmatrix}^k = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ 1 & 0 \end{pmatrix}^k \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^{-1}.$$

Therefore, it follows that

$$\begin{aligned} \begin{pmatrix} x_{n+1} & x_n \\ x_n & x_{n-1} \end{pmatrix} &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} x_{n-1} & x_n \\ x_n & x_{n+1} \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \\ &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ b & a \end{pmatrix}^{n-1} \begin{pmatrix} x_0 & x_1 \\ x_1 & x_2 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \\ &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ 1 & 0 \end{pmatrix}^{n-1} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} x_0 & x_1 \\ x_1 & x_2 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \\ &= \begin{pmatrix} a & b \\ 1 & 0 \end{pmatrix}^{n-1} \begin{pmatrix} x_2 & x_1 \\ x_1 & x_0 \end{pmatrix}. \end{aligned}$$

□

6.2.1 Fibonacci, Lucas, Pell and Pell-Lucas numbers

Here we present the definitions some famous second-order linear sequences.

Fibonacci numbers:	$(F_n)_{n\geq 0}:$	$0,1,1,2,3,5,8,13,21,34,55,89,\ldots.$
Lucas numbers:	$(L_n)_{n\geq 0}:$	$2,1,3,4,7,11,18,29,47,76,123,\ldots.$
Pell numbers:	$(P_n)_{n\geq 0}:$	$0,1,2,5,12,29,70,169,408,985,2378,\ldots.$
Pell-Lucas numbers:	$(Q_n)_{n\geq 0}:$	$2,2,6,14,34,82,198,478,1154,2786,\ldots,$

indexed as A000045, A000032, A000129, and A002203, in the OEIS [211]. Below we present some explicit formulae for the terms of these sequences.

Theorem 6.2. 1° *(Fibonacci numbers) Let F_n be given by $F_0 = 0$, $F_1 = 1$ and*

$$F_{n+2} = F_{n+1} + F_n, \quad n = 0,1,2,\ldots.$$

The formula of the general term is given by

$$F_n = \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right]. \tag{6.11}$$

2° *(Lucas numbers) Let L_n be given by $L_0 = 2$, $L_1 = 1$ and*

$$L_{n+2} = L_{n+1} + L_n, \quad n = 0,1,2,\ldots.$$

The formula of the general term is given by

$$L_n = \left(\frac{1+\sqrt{5}}{2}\right)^n + \left(\frac{1-\sqrt{5}}{2}\right)^n. \tag{6.12}$$

3° *(Pell numbers) Let P_n be given by $P_0 = 0$, $P_1 = 1$ and*

$$P_{n+2} = 2P_{n+1} + P_n, \quad n = 0,1,2,\ldots.$$

The formula of the general term is given by

$$P_n = \frac{1}{2\sqrt{2}}\left[\left(1+\sqrt{2}\right)^n - \left(1-\sqrt{2}\right)^n\right]. \tag{6.13}$$

4° *(Pell-Lucas numbers) Let Q_n be given by $Q_0 = 2$, $Q_1 = 2$ and*

$$Q_{n+2} = 2Q_{n+1} + Q_n, \quad n = 0,1,2,\ldots.$$

The formula of the general term is given by

$$Q_n = \left(1+\sqrt{2}\right)^n + \left(1-\sqrt{2}\right)^n. \tag{6.14}$$

Proof. 1° The associated characteristic equation is

$$t^2 - t - 1 = 0,$$

having the distinct roots $t_1 = \dfrac{1+\sqrt{5}}{2}$ and $t_2 = \dfrac{1-\sqrt{5}}{2}$. Solving the system

$$\begin{cases} c_1 + c_2 = 0 \\ c_1 t_1 + c_2 t_2 = 1, \end{cases}$$

we get $c_1 = \dfrac{1}{\sqrt{5}}$, $c_2 = -\dfrac{1}{\sqrt{5}}$ and the desired formula follows.

2° The proof is similar to that used at 1° for Fibonacci numbers, but now the starting points are instead $L_0 = 2$, $L_1 = 1$.

3° The associated characteristic equation is

$$t^2 - 2t - 1 = 0,$$

having the distinct roots $t_1 = 1 + \sqrt{2}$ and $t_2 = 1 - \sqrt{2}$, while from the initial conditions $P_0 = 0$, $P_1 = 1$ one obtains the formula.

4° The proof follows the same ideas as for Pell numbers, but here we have the starting points $Q_0 = 2$, $Q_1 = 2$. □

These formulae can be extended naturally to negative integers, where they yield the identities

$$F_{-n} = (-1)^{n-1} F_n,\ L_{-n} = (-1)^n L_n,\ P_{-n} = (-1)^{n-1} P_n,\ Q_{-n} = (-1)^n Q_n,$$

valid for all n.

By formula (6.9), one can obtain expressions for the general terms of Fibonacci, Lucas, Pell, and Pell-Lucas sequences, which involve powers of some special matrices.

Theorem 6.3. *The following formulae hold for all integers $n \geq 1$*

$$\begin{pmatrix} F_{n-1} & F_n \\ F_n & F_{n+1} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^{n-1} \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^{n}, \tag{6.15}$$

$$\begin{pmatrix} L_{n-1} & L_n \\ L_n & L_{n+1} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^{n-1} \begin{pmatrix} 2 & 1 \\ 1 & 3 \end{pmatrix}, \tag{6.16}$$

$$\begin{pmatrix} P_{n-1} & P_n \\ P_n & P_{n+1} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix}^{n-1} \begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix}^{n}, \tag{6.17}$$

$$\begin{pmatrix} Q_{n-1} & Q_n \\ Q_n & Q_{n+1} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix}^{n-1} \begin{pmatrix} 2 & 2 \\ 2 & 6 \end{pmatrix}. \tag{6.18}$$

Remark. Using formula (6.10) it follows that for $n \geq 1$ we have

$$\begin{pmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^n;$$
$$\begin{pmatrix} L_{n+1} & L_n \\ L_n & L_{n-1} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^{n-1} \begin{pmatrix} 3 & 1 \\ 1 & 2 \end{pmatrix};$$
$$\begin{pmatrix} P_{n+1} & P_n \\ P_n & P_{n-1} \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}^n;$$
$$\begin{pmatrix} Q_{n+1} & Q_n \\ Q_n & Q_{n-1} \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}^{n-1} \begin{pmatrix} 6 & 2 \\ 2 & 2 \end{pmatrix}.$$

Taking determinants the identities presented in Theorem 6.3, one can obtain the Cassini identities for these sequences.

Theorem 6.4. *The following formulae hold for $n \geq 1$*

$$F_n^2 - F_{n-1}F_{n+1} = (-1)^{n-1} \tag{6.19}$$
$$L_n^2 - L_{n-1}L_{n+1} = 5(-1)^n \tag{6.20}$$
$$P_n^2 - P_{n-1}P_{n+1} = (-1)^{n-1} \tag{6.21}$$
$$Q_n^2 - Q_{n-1}Q_{n+1} = 8(-1)^n. \tag{6.22}$$

Some history and related generalisations of these results are discussed by Melham in [199], or by Fairgrieve and Gould in [113]. For example, the relation (6.19) was apparently proved by Simson in 1753.

We give below an application of the classical Cassini identity.

Example 6.5. *Compute $\sum_{n=1}^{\infty} \frac{(-1)^{n+1}}{F_n F_{n+1}}$, where $(F_n)_{n\geq 0}$ is the Fibonacci sequence.*

Solution. Indeed, by the Cassini relation

$$F_n^2 = F_{n-1}F_{n+1} + (-1)^{n+1},$$

the sum of the first n terms is given by

$$\begin{aligned} S_n &= \sum_{k=1}^{n} \frac{(-1)^{k+1}}{F_k F_{k+1}} = 1 - \sum_{k=2}^{n} \frac{F_{k-1}F_{k+1} - F_k^2}{F_k F_{k+1}} \\ &= 1 - \sum_{k=2}^{n} \left(\frac{F_{k-1}}{F_k} - \frac{F_k}{F_{k+1}} \right) = \frac{F_n}{F_{n+1}}. \end{aligned}$$

Taking limits, the sum of the series is given by

$$\sum_{n=1}^{\infty} \frac{(-1)^{n+1}}{F_n F_{n+1}} = \lim_{n\to\infty} S_n = \frac{2}{1+\sqrt{5}} = \frac{\sqrt{5}-1}{2}.$$

One may consult [3, 145, 170] for more results on reciprocal sums.

Theorem 6.5. 1° *(Golden ratio) The sequence of ratios of Fibonacci numbers*

$$\frac{F_2}{F_1}, \frac{F_3}{F_2}, \frac{F_4}{F_3}, \cdots, \frac{F_{n+1}}{F_n}, \cdots,$$

has the limit $\phi = \frac{1+\sqrt{5}}{2} \approx 1.6180339887\cdots$, *called the* golden ratio.

2° *The sequence of ratios of Lucas numbers*

$$\frac{L_2}{L_1}, \frac{L_3}{L_2}, \frac{L_4}{L_3}, \cdots, \frac{L_{n+1}}{L_n}, \cdots$$

also has the limit $\phi = \frac{1+\sqrt{5}}{2}$.

3° *The sequence of ratios of Pell numbers*

$$\frac{P_2}{P_1}, \frac{P_3}{P_2}, \frac{P_4}{P_3}, \cdots, \frac{P_{n+1}}{P_n}, \cdots,$$

has the limit $1+\sqrt{2}$, *referred to as the* silver ratio.

4° *The sequence of ratios of Pell-Lucas numbers*

$$\frac{Q_2}{Q_1}, \frac{Q_3}{Q_2}, \frac{Q_4}{Q_3}, \cdots, \frac{Q_{n+1}}{Q_n}, \cdots,$$

has the limit $1+\sqrt{2}$.

Proof. 1° From the Binet formula (6.11), we have

$$F_n = \frac{1}{\sqrt{5}} \left[\phi^n - (-1)^n \phi^{-n}\right].$$

One can check that for $n \geq 0$

$$\frac{F_{n+1}}{F_n} = \frac{\phi^{n+1} - (-1)^{n+1}\phi^{-n-1}}{\phi^n - (-1)^n \phi^{-n}}.$$

Clearly, as $\phi > 1$ the limit of this expression is ϕ.

2° From the Binet-type formula (6.12), we have

$$L_n = \phi^n + (-1)^n \phi^{-n},$$

hence

$$\frac{L_{n+1}}{L_n} = \frac{\phi^{n+1} + (-1)^{n+1}\phi^{-n-1}}{\phi^n + (-1)^n \phi^{-n}}.$$

and the solution follows.

3° Similarly, from the Binet-type formula (6.13), we have

$$P_n = \frac{1}{2\sqrt{2}}\left[\alpha^n - (-1)^n\alpha^{-n}\right],$$

where $\alpha = 1+\sqrt{2}$. Therefore,

$$\frac{P_{n+1}}{P_n} = \frac{\alpha^{n+1} - (-1)^{n+1}\alpha^{-n-1}}{\alpha^n - (-1)^n\alpha^{-n}},$$

hence the limit is $\alpha = 1+\sqrt{2}$.

4° By the Binet-type formula (6.14) we have

$$Q_n = \alpha^n + (-1)^n\alpha^{-n},$$

where $\alpha = 1+\sqrt{2}$. We obtain

$$\frac{Q_{n+1}}{Q_n} = \frac{\alpha^{n+1} + (-1)^{n+1}\alpha^{-n-1}}{\alpha^n + (-1)^n\alpha^{-n}},$$

and the conclusion follows. □

Remark. The golden ratio is linked to the proportions between parts of the human body, musical notes and various patterns in nature. Many of these occurrences are presented in the monograph of Koshy [163].

Example 6.6. *Let $(a_n)_{n\geq 0}$ be the sequence defined by $a_0 = 0$, $a_1 = 1$, and*

$$a_{n+1} - 3a_n + a_{n-1} = 2(-1)^n, \quad n = 1,2,\ldots.$$

Prove that a_n is a perfect square for all $n \geq 0$.

Solution. Note that $a_2 = 1$, $a_3 = 4$, $a_4 = 9$, $a_5 = 25$, so $a_0 = F_0^2$, $a_1 = F_1^2$, $a_2 = F_2^2$, $a_3 = F_3^2$, $a_4 = F_4^2$, $a_5 = F_5^2$, where $(F_n)_{n\geq 0}$ is the Fibonacci sequence. We prove that $a_n = F_n^2$ for all $n \geq 0$. Assume that $a_k = F_k^2$ for all $k \leq n$. Hence

$$a_n = F_n^2, \quad a_{n-1} = F_{n-1}^2, \quad a_{n-2} = F_{n-2}^2. \tag{6.23}$$

From the given relation we obtain $a_{n+1} - 3a_n + a_{n-1} = 2(-1)^n$, and

$$a_n - 3a_{n-1} + a_{n-2} = 2(-1)^{n-1}, \quad n \geq 2.$$

Summing up these equalities yields $a_{n+1} - 2a_n - 2a_{n-1} + a_{n-2} = 0$, $n \geq 2$. Using this relation and (6.23) we obtain

$$\begin{aligned} a_{n+1} &= 2F_n^2 + 2F_{n-1}^2 - F_{n-2}^2 = (F_n + F_{n-1})^2 + (F_n - F_{n-1})^2 - F_{n-2}^2 \\ &= F_{n+1}^2 + F_{n-2}^2 - F_{n-2}^2 = F_{n+1}^2. \end{aligned}$$

6.2.2 *Reduction of order*

As shown in [31] and [32], second order linear recurrent sequences can be written as first-order non-linear recurrent sequences.

Theorem 6.6. *The recurrence sequence* (6.3) *satisfies*

$$x_n^2 - ax_nx_{n-1} - bx_{n-1}^2 = (-1)^{n-1}b^{n-1}(\alpha_1^2 - a\alpha_0\alpha_1 - b\alpha_0^2), \quad n = 1,2,\ldots. \tag{6.24}$$

Proof. Taking determinants in both sides in formula (6.9) (or in the relation (6.10)), we obtain the relation

$$x_{n-1}x_{n+1} - x_n^2 = (-b)^{n-1}\left(x_0x_2 - x_1^2\right),$$

which by the recurrence formula (6.3) gives

$$x_{n-1}(ax_n + bx_{n-1}) - x_n^2 = (-b)^{n-1}\left[x_0(ax_1 + bx_0) - x_1^2\right],$$

which represents the relation (6.24). □

From Theorem 6.4, or by applying Theorem 6.6 in the particular case of Fibonacci, Lucas, Pell and Pell-Lucas numbers, one can obtain some other classical results, which connect the sequence terms to just the previous term, but now through a non-linear identity.

Theorem 6.7 (Cassini-type identities). *The following formulae hold for* $n \geq 1$

$$F_n^2 - F_nF_{n-1} - F_{n-1}^2 = (-1)^{n-1} \tag{6.25}$$

$$L_n^2 - L_nL_{n-1} - L_{n-1}^2 = 5(-1)^n \tag{6.26}$$

$$P_n^2 - 2P_nP_{n-1} - P_{n-1}^2 = (-1)^{n-1} \tag{6.27}$$

$$Q_n^2 - Q_nQ_{n-1} - Q_{n-1}^2 = 8(-1)^n. \tag{6.28}$$

Solving the quadratic equations for F_n, L_n, P_n and Q_n in Theorem 6.7, the following first-order non-linear recurrent sequences can be obtained.

Corollary 6.1. *The following relations hold for all integers* $n \geq 1$

$$F_n = \frac{1}{2}\left(F_{n-1} + \sqrt{5F_{n-1}^2 + 4(-1)^{n-1}}\right) \tag{6.29}$$

$$L_n = \frac{1}{2}\left(L_{n-1} + \sqrt{5L_{n-1}^2 + 20(-1)^n}\right) \tag{6.30}$$

$$P_n = P_{n-1} + \sqrt{2P_{n-1}^2 + (-1)^{n-1}} \tag{6.31}$$

$$Q_n = Q_{n-1} + \sqrt{2Q_{n-1}^2 + 8(-1)^n}. \tag{6.32}$$

Extensions involving products of three or more recurrence terms are detailed in [21, Section 2.2]. We here state a Melham-type result without proof.

Theorem 6.8. *Consider the sequence $(x_n)_{n\geq 0}$ defined by the recurrence equation*

$$x_{n+2} = ax_{n+1} + bx_n, \quad n = 0,1,\ldots,$$

with $x_0 = \alpha_0$, $x_1 = \alpha_1$, where α_0, α_1, a, b are given real (or complex) numbers. The following identity holds

$$x_{n+1}x_{n+2}x_{n+6} - x_{n+3}^3 = D(-b)^{n+1}(a^3x_{n+2} - b^2x_{n+1}), \tag{6.33}$$

where $D = a\alpha_0\alpha_1 + b\alpha_0^2 - \alpha_1^2$.

The following Melham-type identities are obtained for Fibonacci, Lucas, Pell and Pell-Lucas numbers. The first of these was given in [199].

Theorem 6.9. *The following formulae hold for $n \geq 1$*

$$F_{n+1}F_{n+2}F_{n+6} - F_{n+3}^3 = (-1)^n F_n \tag{6.34}$$

$$L_{n+1}L_{n+2}L_{n+6} - L_{n+3}^3 = 3(-1)^{n+1} L_n \tag{6.35}$$

$$P_{n+1}P_{n+2}P_{n+6} - P_{n+3}^3 = (-1)^n\,(8P_{n+2} - P_{n+1}) \tag{6.36}$$

$$Q_{n+1}Q_{n+2}Q_{n+6} - Q_{n+3}^3 = 8(-1)^{n+1}\,(8Q_{n+2} - Q_{n+1})\,. \tag{6.37}$$

Example 6.7. *The sequence $(x_n)_{n\geq 1}$ is defined by $x_1 = 0$ and*

$$x_{n+1} = 5x_n + \sqrt{24x_n^2 + 1}, \quad n = 1,2,\ldots.$$

Prove that all x_n are positive integers.

Solution. It is clear that $x_1 < x_2 < \ldots$. The recursive relation is equivalent to

$$x_{n+1}^2 - 10x_nx_{n+1} + x_n^2 - 1 = 0, \quad n = 1,2,\ldots$$

Replacing n by $n-1$ we get

$$x_n^2 - 10x_nx_{n-1} + x_{n-1}^2 - 1 = 0, \quad n = 2,3,\ldots$$

It follows that x_{n+1} and x_{n-1} are the roots of quadratic equation

$$t^2 - 10x_nt + x_n^2 - 1 = 0,$$

hence $x_{n+1} + x_{n-1} = 10x_n$. We obtain

$$x_{n+1} = 10x_n - x_{n-1}, \quad n = 2,3,\ldots, \quad x_1 = 0, x_2 = 1.$$

A simple inductive argument shows that x_n is a positive integer for any n.

6.3 Higher order linear recursions

In this section we present basic results in the theory of linear recurrent sequences. We first discuss the general term for recurrent sequences of higher order defined for arbitrary initial values and recurrence coefficients, based on the article of Andrica and Toader [38] and the monograph of Everest et al. [112]. Some problems where significant progress was made recently are then discussed [214]. The order of a linear recurrence relation can be reduced, as shown by Andrica and Buzeţeanu [31, 32].

Let $m \geq 2$ be a natural number. A **linear recurrence sequence** (LRS) is an infinite sequence $(x_n)_{n\geq 0}$ satisfying the recurrence relation

$$x_n = a_1 x_{n-1} + a_2 x_{n-2} + \cdots + a_m x_{n-m}, \quad m \leq n \in \mathbb{N}. \tag{6.38}$$

If a_i, $i = 1,\ldots,m$ (recurrence coefficients), and α_i, $i = 1,\ldots,m$ (initial conditions) are fixed complex numbers satisfying $a_m \neq 0$ and $x_{i-1} = \alpha_i$, $i = 1,\ldots,m$, then the recurrence relation has order m and is uniquely defined.

The polynomial defined by

$$f(x) = x^m - a_1 x^{m-1} - \cdots - a_{m-1}x - a_m, \tag{6.39}$$

is called the **characteristic polynomial** of the LRS (6.38). The general term of the recursion is given by

$$x_n = P_1(n)z_1^n + \cdots + P_m(n)z_m^n,$$

where $z_1,\ldots,z_m$ are roots of (6.39), and P_i, $i = 1,\ldots,m$ are polynomials in n. If $z_1,\ldots,z_m$ are distinct, then the LRS is **simple** and $P_1,\ldots,P_m$ are constant.

The theory of LRS is a vast subject with extensive applications in mathematics and other sciences. Many properties and results are presented in the monograph of Everest et al. [112]. Decision problems involving LRS with rational terms are discussed by Ouaknine in [214] and other of his papers.
Problem 1 (Skolem). Does $x_n = 0$ for some n?
Problem 2. Is $x_n = 0$ for infinitely many n?
Problem 3 (Positivity). Does $x_n \geq 0$ for all n?
Problem 4 (Ultimate Positivity). Does $x_n \geq 0$ for all but finitely many n?

Berstel and Mignotte showed that Problem 2 is decidable [68]. Ouaknine made progress on Problem 3 for simple LRS of order $m \leq 9$ [215], or arbitrary LRS of order $m \leq 5$ [216], respectively. Problem 4 holds for simple LRS [214].

6.3.1 The general term

Let the sequence $(x_n)_{n\geq 0}$ be defined by the linear recurrence relation (6.38), where $a_1,\ldots,a_m \in \mathbb{C}$, $a_m \neq 0$ and $x_0,\ldots,x_{m-1} \in \mathbb{C}$ are given. We want to find the general term x_n for $n \geq m$. For this we consider the generating function of the sequence $(x_n)_{n\geq 0}$

$$F(z) = x_0 + x_1 z + \cdots + x_n z^n + \cdots. \tag{6.40}$$

The following result presents the relationship between homogeneous linear recurrent sequences and their generating function (see, e.g., [191]).

Theorem 6.10. *Assume that the sequence $(x_n)_{n\geq 0}$ satisfies the homogeneous linear recurrence relation* (6.38)*. The generating function F associated with this sequence can be written as a rational fraction $F(z) = \frac{P(z)}{Q(z)}$, where Q is a polynomial of degree m with nonzero constant term and P is a polynomial of degree strictly less than m.*

Conversely, for any such polynomials P and Q, there exists a unique sequence $(x_n)_{n\geq 0}$ satisfying the linear homogeneous recurrence relation (6.38)*, having the generating function given by the rational function P/Q.*

Proof. From (6.38) and (6.40), the generating function F for the sequence $(x_n)_{n\geq 0}$ can be written as

$$\begin{aligned}
F(z) &= \sum_{j=0}^{m-1} x_j z^j + \sum_{n=m}^{\infty} x_n z^n = \sum_{j=0}^{m-1} x_j z^j + \sum_{n=m}^{\infty} \left(\sum_{j=1}^{m} a_j x_{n-j} \right) z^n \\
&= \sum_{j=0}^{m-1} x_j z^j + \sum_{j=1}^{m} a_j \sum_{n=k}^{\infty} x_{n-j} z^n = \sum_{j=0}^{m-1} x_j z^j + \sum_{j=1}^{m} a_j \sum_{n=m-j}^{\infty} x_n z^{n+j} \\
&= \sum_{j=0}^{m-1} x_j z^j + a_m z^m \sum_{n=0}^{\infty} x_n z^n + \sum_{j=1}^{m-1} a_j z^j \left(\sum_{n=0}^{\infty} x_n z^n - \sum_{i=0}^{m-j-1} x_i z^i \right) \\
&= \sum_{j=0}^{m-1} x_j z^j + F(z) \sum_{j=1}^{m} a_j z^j - \sum_{j=1}^{m-1} a_j z^j \sum_{i=0}^{m-j-1} x_i z^i \\
&= F(z) \sum_{j=1}^{m} a_j z^j + \sum_{j=0}^{m-1} x_j z^j - \sum_{s=1}^{m-1} z^s \sum_{j=1}^{s} a_j x_{s-j}.
\end{aligned}$$

It follows that

$$\begin{aligned}
F(z) \left(1 - \sum_{j=1}^{m} a_j z^j \right) &= \sum_{j=0}^{m-1} x_j z^j - \sum_{s=1}^{m-1} z^s \sum_{j=1}^{s} a_j x_{s-j} \\
&= x_0 + \sum_{s=1}^{m-1} \left(x_s - \sum_{j=1}^{s} a_j x_{s-j} \right) z^s.
\end{aligned}$$

We obtain the polynomials $P \in C_{m-1}[z]$ and $Q \in C_m[z]$ defined by

$$P(z) = x_0 + \sum_{s=1}^{m-1} \left(x_s - \sum_{j=1}^{s} a_j x_{s-j} \right) z^s$$
$$Q(z) = 1 - \sum_{j=1}^{m} a_j z^j.$$

Conversely, if $(x_n)_{n\geq 0}$ is the sequence having the generating function $F(z) = P(z)/Q(z)$, we can write

$$F(z) = \sum_{n=0}^{\infty} x_n z^n, \quad P(z) = \sum_{j=0}^{k} b_j z^j, \quad Q(z) = 1 - \sum_{j=1}^{m} a_j z^j.$$

Clearly, from $F(z) = \frac{P(z)}{Q(z)}$ we obtain the formula

$$\left(1 - \sum_{j=1}^{m} a_j z^j \right) \left(\sum_{n=0}^{\infty} x_n z^n \right) = \sum_{j=0}^{m} b_j z^j.$$

Writing polynomial Q as an infinite series with $a_j = 0$ for $j > m$, we have

$$\sum_{n=0}^{\infty} x_n z^n - \sum_{n=0}^{\infty} \left(\sum_{j=1}^{n} a_j x_{n-j} \right) = \sum_{j=0}^{m} b_j z^j.$$

Identifying the coefficients of z^n, one obtains the recurrence relation

$$x_n = \sum_{j=1}^{m} a_j x_{n-j}, \quad n \geq m.$$

□

Remark. We can write F as a sum of simple fractions. If the polynomial

$$f^*(z) = 1 - a_1 z - \cdots - a_k z^k,$$

has the distinct roots $z_1^*, \ldots, z_m^*$, with multiplicities $q_1, \ldots, q_m$, then

$$F(z) = \frac{P(z)}{f^*(z)} = \sum_{i=1}^{m} \sum_{j=1}^{q_i} \frac{f_{ij}}{\left(z - z_i^*\right)^j}. \tag{6.41}$$

Lemma 6.1. *The coefficients f_{ij} in formula* (6.41) *is*

$$f_{ij} = \frac{1}{(q_i - j)!} \left[(z - z_i^*)^{q_i} F(z) \right]_{z=z_i^*}^{(q_i - j)}, \quad j = 1, \ldots, q_i, \quad i = 1, \ldots, m. \tag{6.42}$$

Proof. By (6.41) we have for $i = 1, \ldots, m$

$$F(z) = \frac{f_{i1}}{z - z_i^*} + \cdots \frac{f_{iq_i}}{\left(z - z_i^*\right)^{q_i}} + h_i(z),$$

or

$$(z - z_i^*)^{q_i} F(z) = f_{i1} (z - z_i^*)^{q_i - 1} + \cdots + f_{iq_i} + (z - z_i^*)^{q_i} h_i(t),$$

which gives (6.42) by successive differentiation. □

Lemma 6.2. *If $u \neq 0$ and $\left|\frac{z}{u}\right| < 1$, then for all integers $j \geq 1$ we have*

$$\frac{1}{(z-u)^j} = (-1)^j u^{-j} \sum_{n \geq 0} \binom{n+j-1}{j-1} \left(\frac{z}{u}\right)^n. \tag{6.43}$$

Proof. The result follows from operations with formal series given in [90], by differentiating the identity below $j - 1$ times with respect to z

$$\frac{1}{z-u} = -\frac{1}{u} \sum_{n \geq 0} \left(\frac{z}{u}\right)^n.$$

□

Theorem 6.11. *The sequence $(x_n)_{n \geq 0}$ defined by* (6.38) *is given by*

$$x_n = P_1(n) z_1^n + \cdots + P_m(n) z_m^n, \quad n \geq k, \tag{6.44}$$

where the $z_1, \ldots, z_m$ are the distinct roots of the polynomial

$$f(z) = z^k - a_1 z^{k-1} - \cdots - a_k,$$

with the orders of multiplicity $q_1, \ldots, q_m$, and

$$P_i(n) = \sum_{j=1}^{q_i} f_{ij} z_i^j \binom{n+j-1}{j-1}, \quad i = 1, \ldots, m. \tag{6.45}$$

Proof. As $z_i = \frac{1}{z_i^*}$, from (6.41) and (6.43) we get

$$\begin{aligned} F(z) &= \sum_{i=1}^{m} \sum_{j=1}^{q_i} \frac{f_{ij}}{\left(z - z_i^*\right)^j} = \sum_{i=1}^{m} \sum_{j=1}^{q_i} \sum_{n \geq 0} (-1)^j f_{ij} z_i^j \binom{n+j-1}{j-1} \left(\frac{z}{z_i^*}\right)^n \\ &= \sum_{n \geq 0} \sum_{i=1}^{m} \sum_{j=1}^{q_i} (-1)^j z_i^{n+j} f_{ij} \binom{n+j-1}{j-1} z^n = \sum_{n \geq 0} \left(\sum_{i=1}^{m} P_i(n) z_i^n \right) z^n, \end{aligned}$$

which is exactly (6.44). □

Example 6.8. *The sequence* $(x_n)_{n\geq 1}$ *is defined as* $x_1 = 20$, $x_2 = 12$ *and*

$$x_{n+2} = x_n + x_{n+1} + 2\sqrt{x_n x_{n+1} + 121}, \quad n \geq 1.$$

1° *Compute* x_{10}*;*
2° *Determine with justification if every term in the sequence is an integer.*

Solution. It is clear that $x_3 = 20 + 12 + 2 \cdot 19 = 70$. Notice that

$$\begin{aligned}
x_{n+3} &= x_{n+1} + x_{n+2} + 2\sqrt{x_{n+1}x_{n+2} + 121} \\
&= x_{n+1} + x_{n+2} + 2\sqrt{x_{n+1}\left(x_n + x_{n+1} + 2\sqrt{x_n x_{n+1} + 121}\right) + 121} \\
&= x_{n+1} + x_{n+2} + 2\sqrt{x_{n+1}^2 + 2\sqrt{x_n x_{n+1} + 121} + x_n x_{n+1} + 121} \\
&= x_{n+1} + x_{n+2} + 2\left(x_{n+1} + \sqrt{x_n x_{n+1} + 121}\right) \\
&= 3x_{n+1} + x_{n+2} + x_{n+2} - x_n - x_{n+1} \\
&= 2x_{n+2} + 2x_{n+1} - x_n.
\end{aligned}$$

Therefore, it follows that $(x_n)_{n\geq 1}$ is an integer sequence and we can compute $x_4 = 144$, $x_5 = 416$, $x_6 = 1010$, $x_7 = 2788$, $x_8 = 7260$, $x_9 = 19046$, $x_{10} = 49824$.

The characteristic equation of $(x_n)_{n\geq 1}$ is $t^3 - 2t^2 - 2t + 1 = 0$, with the roots $t_1 = -1$, $t_2 = \frac{3+\sqrt{5}}{2}$, $t_3 = \frac{3-\sqrt{5}}{2}$. If follows that

$$x_n = c_1(-1)^n + c_2\left(\frac{3+\sqrt{5}}{2}\right)^n + c_3\left(\frac{3-\sqrt{5}}{2}\right)^n, \quad n = 1,2,\ldots.$$

Solving the system $x_1 = 20$, $x_2 = 12$, $x_3 = 70$, we obtain the coefficients

$$c_1 = -\frac{54}{5}, \quad c_2 = \frac{12}{5} + \frac{2\sqrt{5}}{5}, \quad c_3 = \frac{12}{5} - \frac{2\sqrt{5}}{5}.$$

Furthermore, one can write

$$\begin{aligned}
x_n &= \frac{54}{5}(-1)^{n+1} + \frac{1}{5}\left(6 + 6 + 2\sqrt{5}\right)\left(\frac{6+2\sqrt{5}}{4}\right)^n \\
&\quad + \frac{1}{5}\left(6 + 6 - 2\sqrt{5}\right)\left(\frac{6-2\sqrt{5}}{4}\right)^n \\
&= \frac{54}{5}(-1)^{n+1} + \frac{6}{5}L_{2n} + \frac{4}{5}L_{2n+2},
\end{aligned}$$

where L_m is the mth Lucas number.

6.3.2 The space of solutions

A solution of the recurrence equation (6.38) is any function $x : \mathbb{N} \to \mathbb{C}$ with

$$x(n) = a_1 x(n-1) + a_2 x(n-2) + \cdots + a_m x(n-m), \quad n \geq m. \tag{6.46}$$

(The notation $x(n)$ is only used in this section, while for the rest of the chapter the more compact subscript notation x_n is preferred). As each solution is completely determined by m initial conditions $x(0), x(1), \ldots, x(m-1)$, the set containing the solutions of (6.46) forms a vector space V of dimension m over $\mathbb{C}$. The general term of the sequence satisfying the recurrence relation (6.46) is then a linear combination of m functions which form a basis for V.

For $\lambda \neq 0$, the characteristic equation (6.47) is equivalent to

$$\lambda^m = a_1 \lambda^{m-1} + a_2 \lambda^{m-2} + \cdots + a_{m-1}\lambda + a_m.$$

It may be assumed without loss of generality that the order of the recurrence relation can not be reduced, therefore $c_m \neq 0$. For finding a base of the vector space V, one may first check that the functions $w(n) = \lambda^n$ ($\lambda \neq 0$) are a solution of (6.46), whenever λ is a zero of the **characteristic polynomial**

$$f(x) = x^m - a_1 x^{m-1} - a_2 x^{m-2} - \cdots - a_{m-1}x - a_m. \tag{6.47}$$

As a complex polynomial, $f(x)$ has exactly m roots. Examples of bases for V for the cases when the roots of (6.47) are all distinct, all equal, or distinct with arbitrary multiplicities are presented below.

Proposition 6.1. *If the polynomial f (6.47) has m distinct roots $z_1, \ldots, z_m$, then*

$$f_1(n) = z_1^n,\ f_2(n) = z_2^n,\ \ldots,\ f_m(n) = z_m^n,$$

form a basis of the vector space V of solutions for the recurrence relation (6.46).

The proof is based on two facts. First, each function $f_i(n)$ is a solution of (6.46). Second, the Vandermonde determinant involving the first m values $1, z_i, \ldots, z_i^{m-1}$ of each function $f_i(n)$ is non-zero for distinct values $z_1, \ldots, z_m$. A detailed proof is presented in [147, Theorem 1].

Proposition 6.2. *If z is a unique root with multiplicity m of the the polynomial f given by (6.47), then the m sequences*

$$f_1(n) = z^n,\ f_2(n) = nz^n,\ \ldots,\ f_m(n) = n^{m-1}z^n,$$

form a basis of the vector space V of solutions for the recurrence relation (6.46).

The idea of the argument is that a multiple root of polynomial (6.47) is also a root of its derivative. A detailed proof is given in [147, Corollary 1].

Proposition 6.3. *If a characteristic polynomial of a linear recurrence relation of order d has m distinct roots $z_1,\dots,z_m$ having the multiplicities $d_1,\dots,d_m$ (i.e., the degree is $d_1+\cdots+d_m=d$), then the d sequences*

$$f_{ij}(n)=n^{j-1}z_i^n,\quad 1\le i\le m,\quad 1\le j\le d_i, \tag{6.48}$$

form a basis of the vector space V of solutions for the recurrence relation (6.46).

A proof of this results is given in [147, Theorem 2].

6.3.3 Reduction of order for LRS

As suggested by Andrica and Buzeţeanu in 1982 [31], a second order linear recurrence equation can be reduced to a non-linear recurrence equation of the first order (see Theorem 6.6). In particular, such first order formulae obtained for Fibonacci, Lucas, Pell and Pell-Lucas numbers were presented in Theorem 6.7.

Here we present a more general result, concerning the reduction of order for higher order linear recurrence relation, based on results proved by Andrica and Buzeţeanu in 1985 [32]. Specifically, we show that if a sequence $(x_n)_{n\ge 0}$ satisfies a linear recurrence of order $m\ge 2$, then there exists a polynomial relation between any m consecutive terms. This shows that the linear recurrence relation of order m is in fact reduced to a nonlinear recurrence relation of order $m-1$.

Let $m\ge 2$ be an integer and let the sequence $(x_n)_{n\ge 1}$ satisfying

$$x_n=\sum_{r=1}^{m}a_r x_{n-r},\quad n>m, \tag{6.49}$$

where the starting values $x_i=\alpha_i$, and recurrence coefficients a_i, $i=1,\dots,m$, are given real (or complex) numbers such that $a_m\neq 0$.

For $n\ge m$, let us consider the determinant

$$D_n=\begin{vmatrix} x_{n+m-1} & x_{n+m-2} & \dots & x_{n+1} & x_n \\ x_{n+m-2} & x_{n+m-3} & \dots & x_n & x_{n-1} \\ \dots & \dots & \dots & \dots & \dots \\ x_{n+1} & x_n & \dots & x_{n-m+3} & x_{n-m+2} \\ x_n & x_{n-1} & \dots & x_{n-m+2} & x_{n-m+1} \end{vmatrix}, \tag{6.50}$$

for which we can obtain a recursive formula.

Theorem 6.12. *Let $(x_n)_{n\ge 1}$ be a sequence given by* (6.49) *and let D_n be defined by formula* (6.50)*. For any $n\ge m$, the following relation holds*

$$D_n=(-1)^{(m-1)(n-m)}a_m^{n-m}D_m. \tag{6.51}$$

Proof. Following the steps outlined in [159], [194] and [238] (for $m = 2$), we introduce the matrix

$$A_n = \begin{pmatrix} x_{n+m-1} & x_{n+m-2} & \dots & x_{n+1} & x_n \\ x_{n+m-2} & x_{n+m-3} & \dots & x_n & x_{n-1} \\ \dots & \dots & \dots & \dots & \dots \\ x_{n+1} & x_n & \dots & x_{n-m+3} & x_{n-m+2} \\ x_n & x_{n-1} & \dots & x_{n-m+2} & x_{n-m+1} \end{pmatrix}. \tag{6.52}$$

It is easy to see that

$$A_{n+1} = \begin{pmatrix} 0 & 1 & 0 & 0 & \dots & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & \dots & 0 & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & 0 & \dots & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 & 1 \\ a_1 & a_2 & a_3 & a_4 & \dots & a_{m-2} & a_{m-1} & a_m \end{pmatrix} A_n, \tag{6.53}$$

hence

$$A_n = \begin{pmatrix} 0 & 1 & 0 & 0 & \dots & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & \dots & 0 & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & 0 & \dots & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 & 1 \\ a_1 & a_2 & a_3 & a_4 & \dots & a_{m-2} & a_{m-1} & a_m \end{pmatrix}^{n-m} A_m. \tag{6.54}$$

By taking determinants in (6.54), we obtain

$$\Big((-1)^{m-1}a_m\Big)^{n-m} D_m = D_n,$$

for $n \geq m$, which ends the proof. □

Theorem 6.13. *Let $(x_n)_{n\geq 1}$ be a sequence given by* (6.49)*. There is a polynomial function of degree m defined by $F_m : \mathbb{C}^m \to \mathbb{C}$, so that the relation below holds*

$$F_m(x_n, x_{n-1}, \dots, x_{n-m+1}) = (-1)^{(m-1)(n-m)} a_m^{n-m} F_m(\alpha_m, \alpha_{m-1}, \dots, \alpha_1). \tag{6.55}$$

Notice that from the recurrence relation (6.49) one can compute D_m as a function of the known values $\alpha_1, \alpha_2, \dots, \alpha_m$. For the same reason, one can also express D_n as a function of the terms $x_n, x_{n-1}, \dots, x_{n-m+1}$. Thus, there exists a polynomial function of degree m, such that the relation (6.55) is true. If we suppose that the equation (6.55) can be solved with respect to x_n, this results in an expression involving only the terms $x_{n-1}, x_{n-2}, \dots, x_{n-m+1}$. However, the resulting expression is in general very complicated, as shown bellow.

Example 6.9. *For $m = 2$ we obtain*

$$F_2(x,y) = x^2 - a_1xy - a_2y^2, \tag{6.56}$$

and the sequence $(x_n)_{n\geq 1}$ is given by

$$x_n = a_1x_{n-1} + a_2x_{n-2}, \quad n \geq 3,\, x_1 = \alpha_1,\, x_2 = \alpha_2, \tag{6.57}$$

where the relation $F_2(x_n, x_{n-1}) = (-1)^n a_2^{n-2} F_2(\alpha_2, \alpha_1)$ holds. This relation was proved by induction in [58]. Writing the relation explicitly we have

$$(2x_n - a_1x_{n-1})^2 = (a_1^2 + 4a_2)x_{n-1}^2 + 4(-1)^{n-1}a_2^{n-2}\left(a_2\alpha_1^2 + a_1\alpha_1\alpha_2 - \alpha_2^2\right). \tag{6.58}$$

Under some special conditions on $(x_n)_{n\geq 1}$, we can express x_n as an explicit formula of x_{n-1}. Moreover, if the sequence satisfies the second order recurrence equation (6.57) *with a_1, a_2 and α_1, α_2 integers, by* (6.58) *then*

$$(a_1^2 + 4a_2)x_{n-1}^2 + 4(-1)^{n-1}a_2^{n-2}\left(a_2\alpha_1^2 + a_1\alpha_1\alpha_2 - \alpha_2^2\right),$$

is a perfect square. This results extends [151].

Example 6.10. *Simple computations show that for $m = 3$ we have*

$$\begin{aligned} F_3(x,y,z) = &- x^3 - (a_3 + a_1a_2)y^3 - a_3^2z^3 + 2a_1x^2y + a_2x^2z - (a_2^2 + a_1a_3)y^2z \\ &- (a_1^2 - a_2)xy^2 - a_1a_3xz^2 - 2a_2a_3yz^2 + (3a_3 - a_1a_2)xyz. \end{aligned}$$

By (6.55) *we obtain that for the linear recurrence relation*

$$x_n = a_1x_{n-1} + a_2x_{n-2} + a_3x_{n-3}, \quad n \geq 4,\, x_1 = \alpha_1, x_2 = \alpha_2, x_3 = \alpha_3, \tag{6.59}$$

one has the relation $F_3(x_n, x_{n-1}, x_{n-2}) = a_3^{n-3}F_3(\alpha_3, \alpha_2, \alpha_1)$.

Example 6.11. *The Tribonacci numbers are defined by the recurrence relation*

$$T_n = T_{n-1} + T_{n-2} + T_{n-3}, \quad n \geq 4, \tag{6.60}$$

where $T_1 = 1$, $T_2 = 1$ and $T_3 = 2$. In our notation, we have $\alpha_1 = 1$, $\alpha_2 = 1$, $\alpha_3 = 2$, and $a_1 = a_2 = a_3 = 1$. Substituting in Example 6.10, we obtain

$$F_3(x,y,z) = -x^3 - 2y^3 - z^3 + 2x^2y + x^2z - 2y^2z - xz^2 - 2yz^2 + 2xyz.$$

The nonlinear relation satisfied by Tribonacci numbers is

$$F_3(T_n, T_{n-1}, T_{n-2}) = F_3(\alpha_3, \alpha_2, \alpha_1),$$

where $F_3(\alpha_3, \alpha_2, \alpha_1) = -8 - 2 - 1 + 8 + 4 - 2 - 2 - 2 + 4 = -1$.

6.4 The sequences of Lucas and Pell-Lucas polynomials

The Lucas and Pell-Lucas polynomials $U_n, V_n \in \mathbb{Z}[x,y]$, $n = 0,1,\ldots$, are defined by the formulae

$$U_n(x,y) = \frac{x^n - y^n}{x-y}, \tag{6.61}$$

$$V_n(x,y) = x^n + y^n. \tag{6.62}$$

The polynomials U_n and V_n are symmetric and we have $\deg U_n = n-1$, $n = 1,2,\ldots$, and $\deg V_n = n$, $n = 0,1,\ldots$. Also from (6.61) we can extend the sequence $U_n(x,y)$ for $n = 0$, by $U_0(x,y) = 0$.

On the other hand, the sequences $(U_n(x,y))_{n\geq 0}$ and $(V_n(x,y))_{n\geq 0}$ satisfy the same recursive relation of order 2, with different initial values

$$U_{n+2} = (x+y)U_{n+1} - xyU_n, \quad U_0 = 0, U_1 = 1, \tag{6.63}$$

$$V_{n+2} = (x+y)V_{n+1} - xyV_n, \quad V_0 = 2, V_1 = x+y. \tag{6.64}$$

The Fibonacci, Lucas, Pell and Pell-Lucas numbers can be obtained as particular instances of the polynomials U_n and V_n for special pairs of real numbers (x,y) as detailed below

$$F_n = U_n\left(\frac{1+\sqrt{5}}{2}, \frac{1-\sqrt{5}}{2}\right), \quad n = 0,1,\ldots,$$

$$L_n = V_n\left(\frac{1+\sqrt{5}}{2}, \frac{1-\sqrt{5}}{2}\right), \quad n = 0,1,\ldots,$$

$$P_n = U_n\left(1+\sqrt{2}, 1-\sqrt{2}\right), \quad n = 0,1,\ldots,$$

$$Q_n = V_n\left(1+\sqrt{2}, 1-\sqrt{2}\right), \quad n = 0,1,\ldots.$$

The polynomials U_n and V_n have similar algebraic properties as the Fibonacci, Lucas, Pell and Pell-Lucas numbers. For instance, we have the following matrix forms valid for $n = 1,2,\ldots$

$$\begin{pmatrix} U_{n+1} & -xyU_n \\ U_n & -xyU_{n-1} \end{pmatrix} = \begin{pmatrix} x+y & -xy \\ 1 & 0 \end{pmatrix}^n, \tag{6.65}$$

$$\begin{pmatrix} V_{n+1} & -xyV_n \\ V_n & -xyV_{n-1} \end{pmatrix} = \begin{pmatrix} x+y & -xy \\ 1 & 0 \end{pmatrix}^n \begin{pmatrix} x+y & -2xy \\ 2 & -(x+y) \end{pmatrix}, \tag{6.66}$$

which recover the matrix identities for second order recurrent sequences shown in Theorem 6.1, and in particular polynomials obtained for the cases $(x,y) = \left(\frac{1+\sqrt{5}}{2}, \frac{1-\sqrt{5}}{2}\right)$ and $(x,y) = \left(1+\sqrt{2}, 1-\sqrt{2}\right)$, respectively.

6.4.1 Ordinary generating functions of $(U_n)_{n\geq 0}$, $(V_n)_{n\geq 0}$

Using the formulae for U_n and V_n (6.61), one obtains

$$\sum_{n=0}^{\infty} U_n(x,y)z^n = \frac{1}{x-y}\sum_{n=0}^{\infty}(x^n-y^n)z^n \tag{6.67}$$

$$= \frac{1}{x-y}\left(\frac{1}{1-xz}-\frac{1}{1-yz}\right)$$

$$= \frac{z}{(1-xz)(1-yz)} = \frac{z}{1-(x+y)z+(xy)z^2}, \tag{6.68}$$

$$\sum_{n=0}^{\infty} V_n(x,y)z^n = \sum_{n=0}^{\infty}(x^n+y^n)z^n \tag{6.69}$$

$$= \frac{1}{1-xz}+\frac{1}{1-yz}$$

$$= \frac{2-(x+y)z}{1-(x+y)z+(xy)z^2}. \tag{6.70}$$

Substituting for the polynomials given in Section 1.2.3, we obtain the generating functions for special classical polynomials.

The Fibonacci polynomials. Since $f_n(x) = U_n\left(\frac{x+\sqrt{x^2+4}}{2}, \frac{x-\sqrt{x^2+4}}{2}\right)$, we have

$$\sum_{n=0}^{\infty} f_n(x)z^n = \frac{z}{1-xz-z^2}.$$

The Lucas polynomials. Since $l_n(x) = V_n\left(\frac{x+\sqrt{x^2+4}}{2}, \frac{x-\sqrt{x^2+4}}{2}\right)$, we have

$$\sum_{n=0}^{\infty} l_n(x)z^n = \frac{2-xz}{1-xz-z^2}.$$

The Pell polynomials. As $p_n(x) = U_n\left(x+\sqrt{x^2+1}, x-\sqrt{x^2+1}\right)$, we have

$$\sum_{n=0}^{\infty} p_n(x)z^n = \frac{z}{1-2xz-z^2}.$$

The Pell-Lucas polynomials. As $q_n(x) = V_n\left(x+\sqrt{x^2+1}, x-\sqrt{x^2+1}\right)$

$$\sum_{n=0}^{\infty} q_n(x)z^n = \frac{2-2xz}{1-2xz-z^2}.$$

The Chebyshev polynomials of the first kind. Since we have the relation $T_n(x) = \frac{1}{2}V_n\left(x+\sqrt{x^2-1}, x-\sqrt{x^2-1}\right)$, if follows that

$$\sum_{n=0}^{\infty} T_n(x)z^n = \frac{1-2xz}{1-2xz+z^2}.$$

The Chebyshev polynomials of the second kind. Since we have the relation $u_n(x) = U_{n+1}\left(x+\sqrt{x^2-1}, x-\sqrt{x^2-1}\right)$, it follows that

$$\sum_{n=0}^{\infty} u_n(x)z^n = \frac{1}{1-2xz+z^2}.$$

The Hoggatt-Bicknell-King polynomial of Fibonacci kind. Since we have $g_n(x) = U_n\left(\frac{x+\sqrt{x^2-4}}{2}, \frac{x-\sqrt{x^2-4}}{2}\right)$, it follows that

$$\sum_{n=0}^{\infty} g_n(x)z^n = \frac{z}{1-xz+z^2}.$$

The Hoggatt-Bicknell-King polynomial of Lucas kind. By the relation $h_n(x) = V_n\left(\frac{x+\sqrt{x^2-4}}{2}, \frac{x-\sqrt{x^2-4}}{2}\right)$, one has

$$\sum_{n=0}^{\infty} h_n(x)z^n = \frac{2-xz}{1-xz+z^2}.$$

The Jacobsthal polynomials. Since $J_n(x) = U_n\left(\frac{1+\sqrt{8x+1}}{2}, \frac{1-\sqrt{8x+1}}{2}\right)$, we have

$$\sum_{n=0}^{\infty} J_n(x)z^n = \frac{z}{1-z-4xz^2}.$$

The Morgan-Voyce polynomials. As $B_{n-1}(x) = g_n(x+2)$, $g_0(x) = 0$, we get

$$\sum_{n=0}^{\infty} B_n(x)z^n = \sum_{n=0}^{\infty} g_{n+1}(x)z^n = \frac{1}{z}\sum_{n=1}^{\infty} g_n(x+2)z^n = \frac{1}{1-(x+2)z+z^2}.$$

The Brahmagupta polynomials. For the integer parameter $t > 0$ we have $x_n(x,y) = \frac{1}{2}V_n\left(x+y\sqrt{t}, x-y\sqrt{t}\right)$, $y_n(x,y) = yU_n\left(x+y\sqrt{t}, x-y\sqrt{t}\right)$, so

$$\sum_{n=0}^{\infty} x_n(x,y)z^n = \frac{1-xz}{1-2xz+(x^2-y^2t)z^2}$$
$$\sum_{n=0}^{\infty} y_n(x,y)z^n = \frac{yz}{1-2xz+(x^2-y^2t)z^2}.$$

6.4.2 The explicit formula for the Fibonacci, Lucas, Pell and Pell-Lucas polynomials

Using the ordinary generating functions of the Fibonacci, Lucas, Pell and Pell-Lucas polynomials, we can derive the following algebraic expressions.

Theorem 6.14. *For every positive integer n, we have*

$$1^\circ \qquad f_n(x) = \sum_{j=0}^{\lfloor \frac{n-1}{2} \rfloor} \binom{n-j-1}{j} x^{n-2j-1}; \tag{6.71}$$

$$2^\circ \qquad l_n(x) = \sum_{j=0}^{\lfloor \frac{n}{2} \rfloor} \frac{n}{n-j} \binom{n-j}{j} x^{n-2j}; \tag{6.72}$$

$$3^\circ \qquad p_n(x) = \sum_{j=0}^{\lfloor \frac{n-1}{2} \rfloor} \binom{n-j-1}{j} 2^{n-2j-1} x^{n-2j-1}; \tag{6.73}$$

$$4^\circ \qquad q_n(x) = \sum_{j=0}^{\lfloor \frac{n}{2} \rfloor} \frac{n}{n-j} \binom{n-j}{j} 2^{n-2j} x^{n-2j}. \tag{6.74}$$

Proof. 1° Using the geometric series we can write

$$\begin{aligned} \sum_{n=0}^{\infty} f_n(x) z^n &= \frac{z}{1-xz-z^2} = \frac{z}{1-(x+z)z} \\ &= \sum_{m=0}^{\infty} (x+z)^m z^{m+1} \\ &= \sum_{n=0}^{\infty} \left(\sum_{j=0}^{\lfloor \frac{n-1}{2} \rfloor} \binom{n-j-1}{j} x^{n-2j-1} \right) z^n, \end{aligned}$$

and the formula follows by identification of the corresponding coefficients.

2° Following the same idea as before, we have

$$\begin{aligned} \sum_{n=0}^{\infty} l_n(x) z^n &= \frac{2-xz}{1-xz-z^2} = \frac{2-xz}{1-(x+z)z} \\ &= \sum_{m=0}^{\infty} (2-xz)(x+z)^m z^m \\ &= \sum_{n=0}^{\infty} \left(\sum_{j=0}^{\lfloor \frac{n}{2} \rfloor} \frac{n}{n-j} \binom{n-j}{j} x^{n-2j} \right) z^n, \end{aligned}$$

hence the formula (6.72) follows.

3° From the generating function of the Pell numbers, we obtain

$$\begin{aligned}\sum_{n=0}^{\infty} p_n(x)z^n &= \frac{z}{1-2xz-z^2} = \frac{z}{1-(2x+z)z} \\ &= \sum_{m=0}^{\infty} (2x+z)^m z^{m+1} \\ &= \sum_{n=0}^{\infty} \left(\sum_{j=0}^{\lfloor \frac{n-1}{2} \rfloor} \binom{n-j-1}{j} 2^{n-2j-1} x^{n-2j-1} \right) z^n,\end{aligned}$$

and the formula follows by identifying the corresponding coefficients.

4° Analogously, for the Pell-Lucas polynomials, we have

$$\begin{aligned}\sum_{n=0}^{\infty} q_n(x)z^n &= \frac{2-2xz}{1-2xz-z^2} = \frac{2-2xz}{1-(2x+z)z} \\ &= 2\sum_{m=0}^{\infty} (1-xz)(2x+z)^m z^m \\ &= \sum_{n=0}^{\infty} \left(\sum_{j=0}^{\lfloor \frac{n}{2} \rfloor} \frac{n}{n-j} \binom{n-j}{j} 2^{n-2j} x^{n-2j} \right) z^n,\end{aligned}$$

and the desired formula follows. □

As $F_n = f_n(1)$, by (6.71) we obtain the Lucas formula in Theorem 6.14 with a different proof. Similar formulae hold for L_n, P_n and Q_n.

Corollary 6.2. *The following relations hold:*

$$1^\circ \quad F_n = \sum_{j=0}^{\lfloor \frac{n-1}{2} \rfloor} \binom{n-j-1}{j}; \tag{6.75}$$

$$2^\circ \quad L_n = \sum_{j=0}^{\lfloor \frac{n}{2} \rfloor} \frac{n}{n-j} \binom{n-j}{j}; \tag{6.76}$$

$$3^\circ \quad P_n = \sum_{j=0}^{\lfloor \frac{n-1}{2} \rfloor} \binom{n-j-1}{j} 2^{n-2j-1}; \tag{6.77}$$

$$4^\circ \quad Q_n = \sum_{j=0}^{\lfloor \frac{n}{2} \rfloor} \frac{n}{n-j} \binom{n-j}{j} 2^{n-2j}. \tag{6.78}$$

6.4.3 Applications to classical sequences

Using $(x,y) = \left(\frac{1+\sqrt{5}}{2}, \frac{1-\sqrt{5}}{2}\right)$ one obtains the generating functions which correspond to Fibonacci and Lucas sequences. In this case, $xy = -1$ and $x + y = 1$, hence by the formulae (6.67) and (6.69) we have

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

For $(x,y) = \left(1 + \sqrt{2}, 1 - \sqrt{2}\right)$, the generating functions for Pell and Pell-Lucas sequences are obtained. Indeed, here $xy = -1$ and $x + y = 2$, hence by the formulae (6.67) and (6.69) we have

$$\sum_{n=0}^{\infty} P_n z^n = \frac{z}{1 - 2z - z^2}$$
$$\sum_{n=0}^{\infty} Q_n z^n = \frac{2 - 2z}{1 - 2z - z^2}.$$

In many situations, it is possible to obtain the generating function of the sequence $(x_n)_{n\geq 0}$ using only the recurrence relation, and then to derive some properties of the sequence.

We illustrate this idea for second order recurrence relations. Assume that $(x_n)_{n\geq 0}$ is given by $x_{n+2} = ax_{n+1} + bx_n$, $n = 0, 1, \ldots$, where $x_0 = \alpha_0$ and $x_1 = \alpha_1$, while a, b are real (or complex) numbers with $b \neq 0$. We can write

$$\begin{aligned} F(z) &= \sum_{n=0}^{\infty} x_n z^n = x_0 + x_1 z + \sum_{n=2}^{\infty} x_n z^n \\ &= \alpha_0 + \alpha_1 z + \sum_{n=2}^{\infty} (ax_{n-1} + bx_{n-2}) z^n \\ &= \alpha_0 + \alpha_1 z + az\,(F(z) - \alpha_0) + bz^2 F(z), \end{aligned}$$

and obtain the following relation

$$F(z) = \frac{\alpha_0 + (\alpha_1 - a\alpha_0) z}{1 - az - bz^2}. \tag{6.79}$$

From formula (6.79) we can derive the Binet-type formula for the sequence $(x_n)_{n\geq 0}$. Let t_1, t_2 be the roots of the characteristic equation associated to the sequences, $t^2 - at - b = 0$.

Clearly, we have $1 - az - bz^2 = (1 - t_1 z)(1 - t_2 z)$, hence the decomposition of the fraction in (6.79) can be written as

$$\frac{\alpha_0 + (\alpha_1 - a\alpha_0)\, z}{1 - az - bz^2} = \frac{A}{1 - t_1 z} + \frac{B}{1 - t_2 z}, \tag{6.80}$$

where the values of A and B can be determined by identifying the coefficients in the equality $\alpha_0 + (\alpha_1 - a\alpha_0)\, z = A(1 - t_2 z) + B(1 - t_1 z)$. This leads to the system $A + B = \alpha_0$ and $t_2 A + t_1 B = a\alpha_0 - \alpha_1$. If $t_1 \neq t_2$, then we get

$$A = \frac{\alpha_0 t_1 + \alpha_1 - a\alpha_0}{t_1 - t_2}, \quad B = -\frac{\alpha_0 t_2 + \alpha_1 - a\alpha_0}{t_1 - t_2}.$$

We can derive the explicit formula for x_n by expanding the fractions in (6.80) as geometric series, and the comparing coefficients of z^n on either side. It follows that for $n = 0, 1, \ldots$, we have

$$\begin{aligned} x_n &= A t_1^n + B t_2^n \\ &= \frac{1}{t_1 - t_2} \left[(\alpha_0 t_1 + \alpha_1 - a\alpha_0)\, t_1^n - (\alpha_0 t_2 + \alpha_1 - a\alpha_0)\, t_2^n \right]. \end{aligned} \tag{6.81}$$

If $t_1 = t_2$, then it is possible to derive the formula for x_n directly from (6.81), by taking the limit $t_2 \to t_1$. We obtain

$$\begin{aligned} x_n &= \alpha_0 \lim_{t_2 \to t_1} \frac{t_1^{n+1} - t_2^{n+1}}{t_1 - t_2} + (\alpha_1 - a\alpha_0) \lim_{t_2 \to t_1} \frac{t_1^n - t_2^n}{t_1 - t_2} \\ &= \alpha_0 (n+1) t_1^n + + (\alpha_1 - a\alpha_0)\, n t_1^{n-1} \\ &= \left[\alpha_0 t_1 + (\alpha_0 t_1 + \alpha_1 - a\alpha_0)\, n \right] t_1^{n-1}, \quad n = 0, 1, \ldots. \end{aligned}$$

Example 6.12. *Find the recurrence relation satisfied by the sequence $(F_{rn})_{n \geq 0}$, consisting of those Fibonacci numbers whose index is a multiple of r, where r is a fixed positive integer.*

Solution. Denoting $\alpha = \frac{1+\sqrt{5}}{2}$ and $\beta = \frac{1-\sqrt{5}}{2}$, one may write

$$\begin{aligned} \sum_{n=0}^{\infty} F_{rn} z^n &= \sum_{n=0}^{\infty} \frac{1}{\sqrt{5}} (\alpha^{rn} - \beta^{rn})\, z^n \\ &= \frac{1}{\sqrt{5}} \left(\sum_{n=0}^{\infty} \alpha^{rn} z^n - \sum_{n=0}^{\infty} \beta^{rn} z^n \right) \\ &= \frac{1}{\sqrt{5}} \left(\sum_{n=0}^{\infty} (\alpha^r z)^n - (\beta^r z)^n \right) \\ &= \frac{1}{\sqrt{5}} \left(\frac{1}{1 - \alpha^r z} + \frac{1}{1 - \beta^r z} \right). \end{aligned}$$

We also obtain the relation

$$\begin{aligned}\sum_{n=0}^{\infty} F_{rn} z^n &= \frac{1}{\sqrt{5}}\left(\frac{1}{1-\alpha^r z} + \frac{1}{1-\beta^r z}\right)\\ &= \frac{\frac{1}{\sqrt{5}}\left(\alpha^r - \beta^r\right) z}{1-\left(\alpha^r+\beta^r\right) z + (\alpha\beta)^r z^2}\\ &= \frac{F_r z}{1 - L_r z + (-1)^r z^2},\end{aligned}$$

where L_r denotes the rth Lucas number. The denominator leads immediately to the recurrence relation

$$F_{r(n+2)} = L_r F_{r(n+1)} + (-1)^{r+1} F_{r(n-1)}, \quad n = 0,1,\ldots. \tag{6.82}$$

6.4.4 Exponential generating functions of $(U_n)_{n\geq 0}$, $(V_n)_{n\geq 0}$

Using the formulae for the polynomials U_n and V_n (6.61), we have

$$\begin{aligned}\sum_{n=0}^{\infty} \frac{1}{n!} U_n(x,y) z^n &= \frac{1}{x-y} \sum_{n=0}^{\infty} \frac{1}{n!} \left(x^n - y^n\right) z^n\\ &= \frac{1}{x-y}\left[\sum_{n=0}^{\infty} \frac{1}{n!}(xz)^n - \sum_{n=0}^{\infty} \frac{1}{n!}(yz)^n\right] = \frac{e^{xz} - e^{yz}}{x-y}.\end{aligned} \tag{6.83}$$

and

$$\sum_{n=0}^{\infty} \frac{1}{n!} V_n(x,y) z^n = \sum_{n=0}^{\infty} \frac{1}{n!} \left(x^n + y^n\right) z^n = e^{xz} + e^{yz}. \tag{6.84}$$

Here we use the hyperbolic functions $\sinh u = \frac{e^u - e^{-u}}{2}$ and $\cosh u = \frac{e^u + e^{-u}}{2}$.

The Fibonacci polynomials. Since $f_n(x) = U_n\left(\frac{x+\sqrt{x^2+4}}{2}, \frac{x-\sqrt{x^2+4}}{2}\right)$, we have

$$\begin{aligned}\sum_{n=0}^{\infty} \frac{1}{n!} f_n(x) z^n &= \frac{1}{\sqrt{x^2+4}}\left(e^{\frac{x+\sqrt{x^2+4}}{2}\cdot z} - e^{\frac{x-\sqrt{x^2+4}}{2}\cdot z}\right)\\ &= \frac{2e^{\frac{xz}{2}}}{\sqrt{x^2+4}} \frac{e^{\frac{1}{2}z\sqrt{x^2+4}} - e^{-\frac{1}{2}z\sqrt{x^2+4}}}{2} = \frac{2e^{\frac{xz}{2}}}{\sqrt{x^2+4}} \sinh\frac{z\sqrt{x^2+4}}{2}.\end{aligned}$$

The Lucas polynomials. Since $l_n(x) = V_n\left(\frac{x+\sqrt{x^2+4}}{2}, \frac{x-\sqrt{x^2+4}}{2}\right)$, we have

$$\sum_{n=0}^{\infty}\frac{1}{n!}l_n(x)z^n = e^{\frac{x+\sqrt{x^2+4}}{2}\cdot z} + e^{\frac{x-\sqrt{x^2+4}}{2}\cdot z}$$
$$= 2e^{\frac{xz}{2}}\frac{e^{\frac{1}{2}z\sqrt{x^2+4}} + e^{-\frac{1}{2}z\sqrt{x^2+4}}}{2} = 2e^{\frac{xz}{2}}\cosh\frac{z\sqrt{x^2+4}}{2}.$$

The Pell polynomials. As $p_n(x) = U_n\left(x+\sqrt{x^2+1}, x-\sqrt{x^2+1}\right)$, we have

$$\sum_{n=0}^{\infty}\frac{1}{n!}p_n(x)z^n = \frac{2e^{xz}}{\sqrt{x^2+1}}\sinh z\sqrt{x^2+1}.$$

The Pell-Lucas polynomials. As $q_n(x) = V_n\left(x+\sqrt{x^2+1}, x-\sqrt{x^2+1}\right)$

$$\sum_{n=0}^{\infty}\frac{1}{n!}q_n(x)z^n = 2e^{xz}\cosh z\sqrt{x^2+1}.$$

The Chebyshev polynomials of the first kind. Since we have the relation $T_n(x) = \frac{1}{2}V_n\left(x+\sqrt{x^2-1}, x-\sqrt{x^2-1}\right)$, it follows that

$$\sum_{n=0}^{\infty}\frac{1}{n!}T_n(x)z^n = e^{xz}\cosh z\sqrt{x^2-1}.$$

The Chebyshev polynomials of the second kind. We have the relation $u_n(x) = U_{n+1}\left(x+\sqrt{x^2-1}, x-\sqrt{x^2-1}\right)$, while by (6.83) we deduce that

$$\sum_{n=0}^{\infty}\frac{1}{n!}U_{n+1}(x,y)z^n = \frac{xe^{xz}-ye^{yz}}{x-y}.$$

It follows that

$$\sum_{n=0}^{\infty}\frac{1}{n!}u_n(x)z^n = \frac{\left(x+\sqrt{x^2-1}\right)e^{\left(x+\sqrt{x^2-1}\right)z} - \left(x-\sqrt{x^2-1}\right)e^{\left(x-\sqrt{x^2-1}\right)z}}{2\sqrt{x^2-1}}$$
$$= \frac{e^{xz}}{\sqrt{x^2-1}}\left(x\sinh z\sqrt{x^2-1} + \sqrt{x^2-1}\cosh z\sqrt{x^2-1}\right).$$

The Hoggatt-Bicknell-King polynomial of Fibonacci kind. Since we have $g_n(x) = U_n\left(\frac{x+\sqrt{x^2-4}}{2}, \frac{x-\sqrt{x^2-4}}{2}\right)$, it follows that

$$\sum_{n=0}^{\infty}\frac{1}{n!}g_n(x)z^n = \frac{2e^{\frac{xz}{2}}}{\sqrt{x^2-4}}\sinh\frac{z\sqrt{x^2-4}}{2}.$$

The Hoggatt-Bicknell-King polynomial of Lucas kind. By the relation $h_n(x) = V_n\left(\frac{x+\sqrt{x^2-4}}{2}, \frac{x-\sqrt{x^2-4}}{2}\right)$, we have

$$\sum_{n=0}^{\infty} \frac{1}{n!} h_n(x) z^n = 2e^{\frac{xz}{2}} \cosh \frac{z\sqrt{x^2-4}}{2}.$$

The Jacobsthal polynomials. Since $J_n(x) = U_n\left(\frac{1+\sqrt{8x+1}}{2}, \frac{1-\sqrt{8x+1}}{2}\right)$, we have

$$\sum_{n=0}^{\infty} \frac{1}{n!} J_n(x) z^n = \frac{2e^{\frac{z}{2}}}{\sqrt{8x+1}} \sinh \frac{z\sqrt{8x+1}}{2}.$$

The Morgan-Voyce polynomials. Since $B_{n-1}(x) = g_n(x+2)$ and $g_0(x) = 0$, as for Chebysev polynomials of the second kind, one obtains

$$\begin{aligned}\sum_{n=0}^{\infty} \frac{1}{n!} B_n(x) z^n &= \frac{\frac{x+\sqrt{x^2-4}}{2} e^{\frac{x+\sqrt{x^2-4}}{2} z} - \frac{x-\sqrt{x^2-4}}{2} e^{\frac{x-\sqrt{x^2-4}}{2} z}}{\sqrt{x^2-4}} \\ &= \frac{e^{\frac{xz}{2}}}{\sqrt{x^2-4}} \left(x \sinh \frac{z\sqrt{x^2-4}}{2} + \sqrt{x^2-4} \cosh \frac{z\sqrt{x^2-4}}{2} \right).\end{aligned}$$

The Brahmagupta polynomials. For the integer parameter $t > 0$ we have $x_n(x,y) = \frac{1}{2} V_n\left(x + y\sqrt{t}, x - y\sqrt{t}\right)$, $y_n(x,y) = y U_n\left(x + y\sqrt{t}, x - y\sqrt{t}\right)$, so

$$\sum_{n=0}^{\infty} \frac{1}{n!} x_n(x,y) z^n = e^{xz} \cosh yz\sqrt{t}.$$

$$\sum_{n=0}^{\infty} \frac{1}{n!} y_n(x,y) z^n = \frac{e^{xz}}{\sqrt{t}} \sinh yz\sqrt{t}.$$

Substituting $x = 1$ in the formulae for the exponential generating functions for Fibonacci, Lucas, Pell and Lucas Pell polynomials, we obtain

$$\sum_{n=0}^{\infty} \frac{1}{n!} F_n z^n = \frac{2e^{\frac{z}{2}}}{\sqrt{5}} \sinh \frac{z\sqrt{5}}{2};$$

$$\sum_{n=0}^{\infty} \frac{1}{n!} L_n z^n = 2e^{\frac{z}{2}} \cosh \frac{z\sqrt{5}}{2};$$

$$\sum_{n=0}^{\infty} \frac{1}{n!} P_n z^n = \frac{2e^{z}}{\sqrt{2}} \sinh z\sqrt{2};$$

$$\sum_{n=0}^{\infty} \frac{1}{n!} Q_n z^n = 2e^{z} \cosh z\sqrt{2}.$$

6.5 The integral representation of classical sequences

We begin with the integral representation of $U_n(x,y)$, where x,y are nonzero real numbers with $x \neq y$. Assume that $R < \min\left\{\frac{1}{|x|}, \frac{1}{|y|}\right\}$. The ordinary generating function of $U_n(x,y)$ is given in formula (6.67) as

$$\sum_{n=0}^{\infty} U_n(x,y)z^n = \frac{1}{x-y}\sum_{n=0}^{\infty}\left(\frac{1}{1-xz} - \frac{1}{1-yz}\right).$$

The power series in the left hand side is convergent for $|z| < R$, since $|xz| < 1$ and $|yz| < 1$. Applying formula (5.7) we obtain

$$U_n(x,y) = \frac{1}{2\pi(x-y)R^n}\int_0^{2\pi}\left[\frac{\cos nt - i\sin nt}{1-xR(\cos t + i\sin t)} - \frac{\cos nt - i\sin nt}{1-yR(\cos t + i\sin t)}\right]\mathrm{d}t.$$

In order to calculate the first expression in the integral, we have

$$\begin{aligned}\frac{\cos nt - i\sin nt}{1-xR(\cos t + i\sin t)} &= \frac{(\cos nt - i\sin nt)\left[1-xR(\cos t - i\sin t)\right]}{x^2R^2 + 1 - 2xR\cos t}\\ &= \frac{\cos nt - i\sin nt - xR\left[\cos(n+1)t - i\sin(n+1)t\right]}{x^2R^2 + 1 - 2xR\cos t},\end{aligned}$$

and similarly

$$\begin{aligned}\frac{\cos nt - i\sin nt}{1-yR(\cos t + i\sin t)} &= \frac{(\cos nt - i\sin nt)\left[1-yR(\cos t - i\sin t)\right]}{y^2R^2 + 1 - 2xR\cos t}\\ &= \frac{\cos nt - i\sin nt - yR\left[\cos(n+1)t - i\sin(n+1)t\right]}{y^2R^2 + 1 - 2yR\cos t}.\end{aligned}$$

Because $U_n(x,y)$ is a real number, it follows that

$$U_n(x,y) = \frac{1}{2\pi(x-y)R^n}\int_0^{2\pi}\left[\frac{\cos nt - xR\cos(n+1)t}{x^2R^2 + 1 - 2xR\cos t} - \frac{\cos nt - yR\cos(n+1)t}{y^2R^2 + 1 - 2yR\cos t}\right]\mathrm{d}t.$$

After simple computations we obtain the integral formula

$$\begin{aligned}U_n(x,y) &= \frac{1}{2\pi R^{n-1}}\int_0^{2\pi}\frac{xyR^2\cos(n+1)t}{a + b\cos t + c\cos^2 t}\,\mathrm{d}t\\ &- \frac{1}{2\pi R^{n-1}}\int_0^{2\pi}\frac{(x+y)R\cos nt}{a + b\cos t + c\cos^2 t}\,\mathrm{d}t\\ &+ \frac{1}{2\pi R^{n-1}}\int_0^{2\pi}\frac{\cos(n-1)t}{a + b\cos t + c\cos^2 t}\,\mathrm{d}t,\end{aligned} \tag{6.85}$$

where the parameters a, b, c are given by

$$\begin{aligned} a &= a(x,y,R) = (xy)^2R^4 + \left(x^2+y^2\right)R^2 + 1, \\ b &= b(x,y,R) = -2(x+y)(xyR^2+1)R, \\ c &= c(x,y,R) = 4xyR^2. \end{aligned} \tag{6.86}$$

Similarly, the ordinary generating function of $V_n(x,y)$ is given by

$$\sum_{n=0}^{\infty} V_n(x,y)z^n = \frac{1}{1-xz} + \frac{1}{1-yz}.$$

Applying formula (5.7) it follows that

$$V_n(x,y) = \frac{1}{2\pi R^n}\int_0^{2\pi}\left[\frac{\cos nt - xR\cos(n+1)t}{x^2R^2+1-2xR\cos t} + \frac{\cos nt - yR\cos(n+1)t}{y^2R^2+1-2yR\cos t}\right]\mathrm{d}t,$$

hence if a,b,c are defined by (6.86) we obtain

$$\begin{aligned} V_n(x,y) = &\frac{1}{2\pi R^n}\int_0^{2\pi}\frac{2xyR^2\cos(n+2)t}{a+b\cos t+c\cos^2 t}\,\mathrm{d}t \\ &- \frac{1}{2\pi R^n}\int_0^{2\pi}\frac{(x+y)\left(xyR^2+2\right)R\cos(n+1)t}{a+b\cos t+c\cos^2 t}\,\mathrm{d}t \\ &+ \frac{1}{2\pi R^n}\int_0^{2\pi}\frac{\left[(x+y)^2R^2+2\right]\cos nt}{a+b\cos t+c\cos^2 t}\,\mathrm{d}t \\ &- \frac{1}{2\pi R^n}\int_0^{2\pi}\frac{(x+y)R\cos(n-1)t}{a+b\cos t+c\cos^2 t}\,\mathrm{d}t. \end{aligned} \tag{6.87}$$

Remark. Considering the integral

$$I_k = I_k(x,y,R) = \int_0^{2\pi}\frac{\cos kt}{a+b\cos t+c\cos^2 t}\,\mathrm{d}t,$$

formula (6.85) shows that $U_n(x,y)$ is a linear combination of the integrals I_{n+1}, I_n and I_{n-1}, i.e., we have

$$U_n(x,y) = \frac{xy}{2\pi R^{n-3}}I_{n+1} - \frac{x+y}{2\pi R^{n-2}}I_n + \frac{1}{2\pi R^{n-1}}I_{n-1}.$$

Similarly, from (6.87), we obtain $V_n(x,y)$ as the linear combination

$$\begin{aligned} V_n(x,y) = &\frac{xy}{\pi R^{n-2}}I_{n+2} - \frac{(x+y)\left(xyR^2+2\right)}{2\pi R^{n-1}}I_{n+1} \\ &+ \frac{(x+y)^2R^2+2}{2\pi R^n}I_n - \frac{x+y}{2\pi R^{n-1}}I_{n-1}. \end{aligned}$$

Integral formula for Fibonacci numbers

Because $F_n = U_n\left(\frac{1+\sqrt{5}}{2}, \frac{1-\sqrt{5}}{2}\right)$, for Fibonacci numbers we have $x + y = 1$ and $xy = -1$, therefore

$$F_n = \frac{1}{2\pi R^{n-1}} \int_0^{2\pi} \frac{-R^2\cos(n+1)t - R\cos nt + \cos(n-1)t}{R^4 + 3R^2 + 1 + 2(R^3 - R)\cos t - 4R^2\cos^2 t}\,\mathrm{d}t, \quad (6.88)$$

for every positive real number $R < \min\left\{\frac{2}{1+\sqrt{5}}, \frac{2}{\sqrt{5}-1}\right\} = \frac{2}{1+\sqrt{5}} = \frac{\sqrt{5}-1}{2}$.

Using the notation

$$\begin{aligned} I_k &= I_k\left(\frac{1+\sqrt{5}}{2}, \frac{1-\sqrt{5}}{2}, R\right) \\ &= \int_0^{2\pi} \frac{\cos kt}{R^4 + 3R^2 + 1 + 2(R^3 - R)\cos t - 4R^2\cos^2 t}\,\mathrm{d}t, \end{aligned}$$

this can be further written as

$$F_n = -\frac{1}{2\pi R^{n-3}} I_{n+1} - \frac{1}{2\pi R^{n-2}} I_n + \frac{1}{2\pi R^{n-1}} I_{n-1}.$$

Integral formula for Lucas numbers

Because $L_n = V_n\left(\frac{1+\sqrt{5}}{2}, \frac{1-\sqrt{5}}{2}\right)$, and $x^2 + y^2 = 3$, we obtain the following integral formula for Lucas numbers

$$\begin{aligned} L_n = &- \frac{1}{\pi R^{n-2}} \int_0^{2\pi} \frac{\cos(n+2)t}{R^4 + 3R^2 + 1 + 2(R^3 - R)\cos t - 4R^2\cos^2 t}\,\mathrm{d}t \\ &+ \frac{R^2 - 2}{2\pi R^{n-1}} \int_0^{2\pi} \frac{\cos(n+1)t}{R^4 + 3R^2 + 1 + 2(R^3 - R)\cos t - 4R^2\cos^2 t}\,\mathrm{d}t \\ &+ \frac{R^2 + 2}{2\pi R^n} \int_0^{2\pi} \frac{\cos nt}{R^4 + 3R^2 + 1 + 2(R^3 - R)\cos t - 4R^2\cos^2 t}\,\mathrm{d}t \\ &- \frac{1}{2\pi R^{n-1}} \int_0^{2\pi} \frac{\cos(n-1)t}{R^4 + 3R^2 + 1 + 2(R^3 - R)\cos t - 4R^2\cos^2 t}\,\mathrm{d}t, \quad (6.89) \end{aligned}$$

for every positive real number $R < \min\left\{\frac{2}{1+\sqrt{5}}, \frac{2}{\sqrt{5}-1}\right\} = \frac{2}{1+\sqrt{5}} = \frac{\sqrt{5}-1}{2}$.

With the I_k's used for Fibonacci numbers, for Lucas numbers we have

$$L_n = -\frac{1}{\pi R^{n-2}} I_{n+2} + \frac{R^2 - 2}{2\pi R^{n-1}} I_{n+1} + \frac{R^2 + 2}{2\pi R^n} I_n - \frac{1}{2\pi R^{n-1}} I_{n-1}.$$

Integral formula for Pell numbers

Because $P_n = U_n\left(1+\sqrt{2}, 1-\sqrt{2}\right)$, for Pell numbers we have $x+y=2$ and $xy=-1$, therefore

$$P_n = \frac{1}{2\pi R^{n-1}} \int_0^{2\pi} \frac{-R^2\cos(n+1)t - 2R\cos nt + \cos(n-1)t}{R^4+6R^2+1+4(R^3-R)\cos t - 4R^2\cos^2 t}\,\mathrm{d}t, \quad (6.90)$$

for every positive real number $R < \min\left\{\frac{1}{1+\sqrt{2}}, \frac{1}{\sqrt{2}-1}\right\} = \sqrt{2}-1$.

Using the notation

$$\begin{aligned} I_k &= I_k\left(1+\sqrt{2}, 1-\sqrt{2}, R\right) \\ &= \int_0^{2\pi} \frac{\cos kt}{R^4+6R^2+1+4(R^3-R)\cos t - 4R^2\cos^2 t}\,\mathrm{d}t, \end{aligned}$$

we have

$$P_n = -\frac{1}{2\pi R^{n-3}} I_{n+1} - \frac{1}{\pi R^{n-2}} I_n + \frac{1}{2\pi R^{n-1}} I_{n-1}.$$

Integral formula for Pell-Lucas numbers

As $Q_n = V_n\left(1+\sqrt{2}, 1-\sqrt{2}\right)$ and $x^2+y^2=6$, for Pell-Lucas numbers we get the following formula

$$\begin{aligned} Q_n = &-\frac{1}{\pi R^{n-2}} \int_0^{2\pi} \frac{\cos(n+2)t}{R^4+6R^2+1+4(R^3-R)\cos t - 4R^2\cos^2 t}\,\mathrm{d}t \\ &+ \frac{R^2-2}{\pi R^{n-1}} \int_0^{2\pi} \frac{\cos(n+1)t}{R^4+6R^2+1+4(R^3-R)\cos t - 4R^2\cos^2 t}\,\mathrm{d}t \\ &+ \frac{2R^2+1}{\pi R^n} \int_0^{2\pi} \frac{\cos nt}{R^4+6R^2+1+4(R^3-R)\cos t - 4R^2\cos^2 t}\,\mathrm{d}t \\ &- \frac{1}{\pi R^{n-1}} \int_0^{2\pi} \frac{\cos(n-1)t}{R^4+6R^2+1+4(R^3-R)\cos t - 4R^2\cos^2 t}\,\mathrm{d}t, \quad (6.91) \end{aligned}$$

for every positive real number $R < \min\left\{\frac{1}{1+\sqrt{2}}, \frac{1}{\sqrt{2}-1}\right\} = \sqrt{2}-1$.

With the I_k's used for Pell numbers, for Pell-Lucas numbers we have

$$Q_n = -\frac{1}{\pi R^{n-2}} I_{n+2} + \frac{R^2-2}{\pi R^{n-1}} I_{n+1} + \frac{2R^2+1}{\pi R^n} I_n - \frac{1}{\pi R^{n-1}} I_{n-1}.$$

Chapter 7
Polynomials in Multiple Variables

Polynomials in several variables with coefficients in a field K can be defined inductively. To be precise, a polynomial $f(X,Y)$ in two variables X,Y is a polynomial in Y with coefficients in $K[X]$. That means

$$f(X,Y)=\sum_{j=0}^{n} f_j(X)Y^j,$$

where $f_j(X)\in K[X]$. If we write

$$f_j(X)=\sum_{i=0}^{n(j)} a_{ij}X^i$$

we see that $f(X,Y)$ can be expressed as

$$f(X,Y)=\sum_{i,j=0}^{n} a_{ij}X^iY^j,$$

where $n=\max\{n(j)\}$. We will write $f(X,Y)=\sum_{ij}a_{ij}X^iY^j$ and we always assume that this sum is finite. We denote by $K[X,Y]$the set of polynomials in variables X,Y with coefficients in K. It is clear that we can perform addition and multiplication of polynomials in two variables such that $K[X,Y]$ is a ring. Nevertheless, the Euclidean division theorem is not valid unless the divisor is a monic polynomial in one of the variables. For example:

$$X^nY-X^{n-2}Y^2+X^2Y^2+X=\left(X^2-Y\right)\left(X^{n-2}Y+Y^2\right)+X+Y^3,$$

when we divide the polynomial by X^2-Y. But, dividing to $Y-X^2$ we get:

$$X^nY-X^{n-2}Y^2+X^2Y^2+X=\left(Y-X^2\right)\left(-X^{n-2}Y+X^2Y+X^4\right)+X^6+X.$$

Assume that the ring of polynomials in $n-1$ variables $K[X_1,\dots,X_{n-1}]$ is defined. Then, by induction we define

$$K[X_1,\dots,X_n] = K[X_1,\dots,X_{n-1}][X_n].$$

Clearly, a polynomial in the variables $X_1,\dots,X_{n-1},X_n$ is a polynomial in the variable X_n with coefficients polynomials in the variables $X_1,\dots,X_{n-1}$. Such a polynomial is commonly denoted as $F(X_1,\dots,X_n)$. Also, a polynomial in n variables $F(X_1,\dots,X_n)$ can be expressed as a finite formal sum

$$F(X_1,\dots,X_n) = \sum_{I=(i_1,\dots,i_n)} a_i X_1^{i_1}\dots X_n^{i_n},$$

where $I=(i_1,\dots,i_n)$ is an ordered sequence of non negative integers and a_I are constants from one of the number sets $\mathbb{Z},\mathbb{Q},\mathbb{R},\mathbb{C}$ or from $\mathbb{F}_p$.

The product $a_I X_1^{i_1}\dots X_n^{i_n}$ is called a **monomial**. The **degree of the monomial** $a_I X_1^{i_1}\dots X_n^{i_n}$ is $i_1+\dots+i_n$. The degree of a polynomial is the highest degree of its non zero monomials.

To be precise, we defined the **degree of** F by

$$\deg(F) = \max\left\{\deg(X_1^{i_1}\dots X_n^{i_n}) :\ a_{i_1\dots i_n}\neq 0\right\}.$$

This maximum may be attained in more monomials. For example, the polynomial $F=X^3Y-2YZ^5+3X^3Z$ has three variables X, Y and Z, and the degree $\deg(F)=6$.

A polynomial $F(X_1,\dots,X_n)$ is **homogeneous** if all its non zero monomials have the same degree. A homogeneous polynomial of degree 1 is called a linear form and can be written as $a_1X_1+\dots+a_nX_n$, where $a_1,\dots,a_n\in K$.

A general homogeneous polynomial of degree 2 is called a **quadratic form** and can be written as

$$a_1X_1^2+\dots+a_nX_n^2+a_{12}X_1X_2+a_{13}X_1X_3+\dots+a_{n-1,n}X_{n-1}X_n,$$

where $a_i,a_{i,j}\in K$ for all $i,j\in\{0,1,\dots,n\}$.

The following properties hold for homogeneous polynomials.

1) The sum of two homogeneous polynomials **of the same degree** is also a homogeneous polynomial.
2) The product of two homogeneous polynomial is also a homogeneous polynomial.
3) Let f and g be two homogeneous polynomials with f divisible by g. Then, the quotient of f by g is also a homogeneous polynomial.

7.1 Symmetric polynomials

The polynomial $F(X_1,\dots,X_n)$ is said to be symmetric if for any permutation $s=(s_1,\dots,s_n)$ of the set $\{1,2,\dots,n\}$ one has $F(X_1,\dots,X_n)=F(X_{s_1},\dots,X_{s_n})$.

For example, the polynomial $F=X^2Y+XY^2+Y^2Z+YZ^2+Z^2X+ZX^2$ is a symmetric polynomial in three variables. For all $k\geq 1$, the polynomials $P_k(X_1,\dots,X_n)=X_1^k+\cdots+X_n^k$ are symmetric in n variables are symmetric.

Clearly, the polynomial $G=X^2Y-XY^2+Y^2Z-YZ^2+Z^2X-ZX^2$, in three variables, is not symmetric.

Let us consider the following important symmetric polynomials

$$\begin{aligned}
S_1(X_1,\dots,X_n)&=X_1+\cdots+X_n\\
&\dots\\
S_k(X_1,\dots,X_n)&=\sum_{i_1,\dots,i_k}X_{i_1}\cdots X_{i_k}\\
&\dots\\
S_n(X_1,\dots,X_n)&=X_1X_2\dots X_n,
\end{aligned}$$

where the sum in the definition of the term S_k is taken over all k element subsets $\{i_1,\dots,i_k\}$ of the set $\{1,2,\dots,n\}$. By extension for $k>n$, we define $S_k=0$ and also $S_0=1$. These polynomials are generally called the **fundamental symmetric polynomials** in n variables. We will use them throughout the book and for simplicity we denote them by $S_1,\dots,S_n$.

Some properties involving symmetric polynomials in the same variables, analogous to the properties 1) – 3) listed for homogeneous polynomials.

1) The sum of two symmetric polynomials is also a symmetric polynomial.
2) The product of two symmetric polynomials is also a symmetric polynomial.
3) Let f and g be two symmetric polynomials such that f is divisible by g. Then, the quotient is also a symmetric polynomial.

In other words, an algebraic combination of symmetric polynomials is a symmetric polynomial. In numerous applications, the polynomials involved are symmetric and homogeneous, therefore one can make use of the three properties listed above. We now present some illustrative examples.

Example 7.1. *Factorize the polynomial*

$$P(a,b,c)=(b-c)(-2a+b+c)^2+(c-a)(a-2b+c)^2+(a-b)(a+b-2c)^2.$$

Solution. Clearly, P is a symmetric and homogeneous polynomial of degree 3 in a,b,c. Note that $P(a,a,c)=0$, hence P is divisible by $a-b$. Because of the symmetry, P is also divisible by $b-c$ and by $c-a$.

It follows that

$$P(a,b,c) = k(a-b)(b-c)(c-a),$$

for some constant k. Taking $a=0$, $b=1$, $c=2$, we get $P(0,1,2)=2k$, hence $2k=-18$. It follows $k=-9$, so

$$P(a,b,c) = -9(a-b)(b-c)(c-a).$$

A similar example problem is the following.

Example 7.2. *Factorize the expression*

$$E(a,b,c) = (a-b)(a+b)^4 + (b-c)(b+c)^4 + (c-a)(c+a)^4.$$

Solution. It is clear that E is a symmetric and homogeneous polynomial in a,b,c of degree 5. From $E(a,a,c)=0$ it follows that E is divisible by $a-b$ and because the symmetry, E is also divisible by $b-c$ and by $c-a$.

We now get the expression

$$E = (a-b)(b-c)(c-a)\cdot G,$$

where G is a symmetric and homogeneous polynomial of degree 2 in he variables a,b,c. We have

$$G = k_1\left(a^2+b^2+c^2\right) + k_2\left(ab+bc+ca\right),$$

for some constants k_1 and k_2. Therefore

$$E = (a-b)(b-c)(c-a)\left[k_1\left(a^2+b^2+c^2\right) + k_2\left(ab+bc+ca\right)\right].$$

From the relations

$$E(0,1,2) = 2(5k_1+2k_2), \quad E(-1,0,1) = 2(2k_1-k_2),$$

one obtains the system

$$\begin{cases} 5k_1+2k_2 = -25 \\ 2k_1-k_2 = -1, \end{cases}$$

from where it follows that $k_1=-3$ and $k_2=-5$. We get

$$E(a,b,c) = -(a-b)(b-c)(c-a)\left[3\left(a^2+b^2+c^2\right) + 5\left(ab+bc+ca\right)\right].$$

Let us see how these ideas can be used to prove an identity of cyclic form.

Example 7.3. *Prove the identity*

$$\sum_{cyc} x^4(y-z) = -(x-y)(y-z)(z-x)\left(x^2+y^2+z^2+xy+yz+zx\right).$$

Solution. We proceed as in previous problem in order to factor

$$F(x,y,z) = \sum_{cyc} x^4(y-z).$$

It is clear that F is a symmetric and homogeneous polynomial in x,y,z of degree 5. From $F(x,x,z)=0$ it follows that F is divisible by $x-y$, and because the symmetry it is also divisible by $y-z$ and $z-x$. We get

$$F = (x-y)(y-z)(z-x)\cdot H,$$

where H is a symmetric and homogeneous polynomial in x,y,z of degree 2, given by the formula

$$H = k_1\left(x^2+y^2+z^2\right) + k_2\left(xy+yz+zx\right),$$

where k_1 and k_2 are constants to be determined.

From the relations $F(0,1,2) = 2(5k_1+2k_2)$ and $F(-1,0,1) = 2(2k_1-k_2)$, and we obtain the system of equations

$$\begin{cases} 5k_1+2k_2 = -7 \\ 2k_1-k_2 = -1, \end{cases}$$

hence $k_1 = k_2 = -1$, and the conclusion follows.

Second solution. If we provide the substitutions

$$x = b+c, \quad y = c+a, \quad z = a+b,$$

then the left-hand side of the identity is

$$(a-b)(a+b)^4 + (b-c)(b+c)^4 + (c-a)(c+a)^4.$$

Now, we replace x,y,z in the right-hand side and get

$$-(a-b)(b-c)(c-a)\left[3\left(a^2+b^2+c^2\right)+5\left(ab+bc+ca\right)\right].$$

The result now follows from the previous example.

Example 7.4. *Prove the identity*

$$\sum_{cyc}(y-z)(-x+y+z)^3 = -4(x-y)(y-z)(z-x)(x+y+z).$$

Solution. Consider the expression

$$E(x,y,z) = \sum_{cyc}(y-z)(-x+y+z)^3$$

and note that $E(x,x,z) = 0$. It follows that E is divisible by $x-y$, and because the symmetry, it is also divisible by $y-z$ and $z-x$. Taking into account that E is a symmetric and homogeneous polynomial in x,y,z of degree 2, we have the formula

$$E = (x-y)(y-z)(z-x)\cdot F,$$

where F is polynomial in x,y,z of degree 1, both symmetric and homogeneous, hence $F = k(x+y+z)$, for some constant k. From $F(0,1,2) = 6k$, we get $-24 = 6k$, hence $k = -4$ and we are done.

Example 7.5. *Factorize the expression*

$$P(x,y,z) = (x-y)^5 + (y-z)^5 + (z-x)^5.$$

Solution. We have $P(x,x,z) = 0$, $P(x,y,x) = 0$ and $P(x,y,y) = 0$, hence P is divisible by $(x-y)(y-z)(z-x)$. We get

$$P = (x-y)(y-z)(z-x)\cdot Q,$$

where Q is a homogeneous polynomial of degree 2 in x,y,z, hence

$$Q = k_1\left(x^2+y^2+z^2\right) + k_2(xy+yz+zx),$$

where the constants k_1 and k_2 must be determined.

From the relations $P(0,1,2) = 2(5k_1+2k_2)$ and $P(-1,0,1) = 2(2k_1-k_2)$ we obtain the system of equations

$$\begin{cases} 5k_1+2k_2 = 15 \\ 2k_1-k_2 = 15, \end{cases}$$

hence $k_1 = 5$ and $k_2 = -5$. It follows the factorization

$$P(x,y,z) = 5(x-y)(y-z)(z-x)\left(x^2+y^2+z^2-xy-yz-zx\right).$$

Example 7.6. *Factorize the expression*

$$f(x,y,z) = (x+y+z)^3 - (-x+y+z)^3 - (x-y+z)^3 - (x+y-z)^3.$$

Solution. Clearly, f is a symmetric and homogeneous polynomial of degree 3 in x,y,z. Note that $f(0,y,z) = 0$, hence f is divisible by x. Also, we have $f(x,0,z) = f(x,y,0) = 0$, hence f is divisible by y and by z.

It follows that f is divisible by xyz and since $\deg(f) = 3$, we get $f = kxyz$, for some constant k. In order to determine k, observe that $f(1,1,1) = k$, hence $k = 24$. Finally, $f(x,y,z) = 24xyz$.

Example 7.7. *Factorize*

$$g(x,y,z) = (x+y+z)^4 - (x+y)^4 - (y+z)^4 - (z+x)^4 + (x^4+y^4+z^4).$$

Solution. The polynomial g is symmetric in x,y,z and $\deg(g) = 4$. We have

$$g(0,y,z) = g(x,0,z) = g(x,y,0) = 0,$$

hence g is divisible by xyz. It follows that $g = xyz \cdot h$, where h is a symmetric polynomial in x,y,z of degree 1, that is $h = k(x+y+z)$ for some constant k. We get the factorization

$$g = kxyz(x+y+z).$$

In order to find the constant k we set $x = y = z = 1$ and obtain $g(1,1,1) = 3k$, hence $3^4 - 3 \cdot 2^4 + 3 = 3k$. It follows $k = 27 - 16 + 1 = 12$, therefore

$$g = 12xyz(x+y+z).$$

Example 7.8. *Factorize*

$$h(x,y,z) = (x+y+z)^5 - (-x+y+z)^5 - (x-y+z)^5 - (x+y-z)^5.$$

Solution. It is clear that h is a symmetric and homogeneous polynomial in x,y,z of degree 5. From

$$h(0,y,z) = h(x,0,z) = h(x,y,0) = 0,$$

it follows that h is divisible by xyz, hence $h = xyz \cdot g$, where g is a symmetric and homogeneous polynomial of degree 2. We have

$$g = k_1\left(x^2+y^2+z^2\right) + k_2(xy+yz+zx),$$

for some constants k_1 and k_2. Therefore

$$h = xyz\left[k_1\left(x^2+y^2+z^2\right)+k_2\left(xy+yz+zx\right)\right].$$

From the relation

$$h(1,1,1) = 3(k_1+k_2), \quad h(1,2,-1) = -2(6k_1-k_2),$$

it follows the system

$$\begin{cases} k_1+k_2 = 80 \\ 6k_1-k_2 = 6\cdot 80. \end{cases}$$

We get $k_1 = 80$ and $k_2 = 0$, hence

$$h = 80xyz\left(x^2+y^2+z^2\right).$$

Example 7.9. *Factorize*

$$f(x,y,z) = (x+y+z)^5 - x^5 - y^5 - z^5.$$

Solution. The polynomial f is symmetric and homogeneous in x,y,z and $\deg(f) = 5$. We have

$$f(x,-x,z) = f(x,y,-x) = f(x,y,-y) = 0,$$

hence f is divisible by $(x+y)(y+z)(z+x)$. It follows that

$$f = (x+y)(y+z)(z+x)g,$$

where g is a degree 2 polynomial in x,y,z, symmetric and homogeneous, i.e.,

$$g = k_1\left(x^2+y^2+z^2\right)+k_2\left(xy+yz+zx\right),$$

for some constants k_1 and k_2, hence

$$f = (x+y)(y+z)(z+x)\left[k_1\left(x^2+y^2+z^2\right)+k_2\left(xy+yz+zx\right)\right].$$

From the relations $f(1,1,1) = 24(k_1+k_2)$, $f(0,1,2) = 6(5k_1+2k_2)$, we get

$$\begin{cases} k_1+k_2 = 10 \\ 5k_1+2k_2 = 35, \end{cases}$$

hence $k_1 = k_2 = 5$. We get

$$f = 5(x+y)(y+z)(z+x)\left(x^2+y^2+z^2+xy+yz+zx\right).$$

Example 7.10. *Factorize*

$$E(a,b,c) = a^4\left(b^2-c^2\right) + b^4\left(c^2-a^2\right) + c^4\left(a^2-b^2\right).$$

Solution. Denote $a^2 = x$, $b^2 = y$, $c^2 = z$ and consider the symmetric and homogeneous polynomial of degree 3

$$E(x,y,z) = x^2(y-z) + y^2(z-x) + z^2(x-y).$$

It is clear that

$$E_1(x,x,z) = E_1(x,y,x) = E_1(x,y,y) = 0,$$

hence E_1 is divisible by $(x-y)(y-z)(z-x)$. It follows

$$E_1(x,y,z) = k(x-y)(y-z)(z-x),$$

for some constant k. We have $E_1(0,1,2) = 2k$, that is $-2 = 2k$, hence $k = -1$. We get the factorization

$$E(a,b,c) = -\left(a^2-b^2\right)\left(b^2-c^2\right)\left(c^2-a^2\right).$$

We now present a result with deep implications in various areas of mathematics.

Theorem 7.1 (Fundamental theorem of symmetric polynomials). *For every symmetric polynomial $F(X_1,\ldots,X_n)$ there exists a polynomial $G(X_1,\ldots,X_n)$ such that $F(X_1,\ldots,X_n) = G(S_1,\ldots,S_n)$. Moreover, the polynomial G is unique.*

Proof. The proof of this theorem is by double induction. One induction is on the number of variables n and the second on the degree of the polynomial F. The result holds trivially when $n = 1$. Assume the conclusion holds for all symmetric polynomials in $n-1$ variables. Using induction, we are going to prove that it also holds for any symmetric polynomial F in n variables.

Now we induct on $\deg F$, the degree of the polynomial F. It is not hard to verify that the conclusion follows if $\deg F \in \{0,1\}$. Assume that the conclusion holds for all polynomials in at most n variables whose degree is strictly less than that of F.

Define the polynomial in $n-1$ variables

$$g(X_1,\ldots,X_{n-1}) = F(X_1,\ldots,X_{n-1},X_n).$$

The polynomial g is symmetric, because F is. Using the hypothesis of the induction on n, we deduce that there exists h such that

$$g(X_1,X_2,\ldots,X_{n-1}) = h(X_1+X_2+\cdots+X_{n-1},\ldots,X_1X_2\cdots X_n).$$

We now define the polynomial $H \in R[X_1, \ldots, X_n]$ by

$$H(X_1, X_2, \ldots, X_n) = F(X_1, X_2, \ldots, X_n) - h(S_1, S_2, \ldots, S_{n-1}),$$

where S_i, $i = 1, \ldots, n-1$ are the fundamental symmetric polynomials in n variables. Note that H is symmetric. Moreover, as $H(X_1, , X_2, \ldots, X_{n-1}, 0) = 0$ we deduce that $X_n \mid H(X_1, X_2, \ldots, X_n)$. By symmetry it follows that we have $X_1 X_2 \ldots X_n \mid H(X_1, X_2, \ldots, X_n)$. Now, observe that the polynomial

$$\frac{H(X_1, X_2, \ldots, X_n)}{X_1 X_2 \cdots X_n}$$

is symmetric and

$$\deg \left(\frac{H(X_1, X_2, \ldots, X_n)}{X_1 X_2 \cdots X_n} \right) < \deg F.$$

Using the hypothesis of the induction on $\deg F$, it follows that $\frac{H(X_1, X_2, \ldots, X_n)}{X_1 X_2 \cdots X_n}$ can be written as a polynomial expression in the fundamental symmetric polynomials $S_1, S_2, \ldots, S_n$. Now the conclusion follows easily for F and both inductions are complete. □

For example, we can write the expressions

$$\begin{aligned} S_1^2 - 2S_2 &= X_1^2 + \cdots + X_n^2 \\ S_1 S_2 - 3S_3 &= (X + Y + Z)(XY + YZ + ZX) - 3XYZ \\ &= X^2 Y + XY^2 + Y^2 Z + YZ^2 + Z^2 X + ZX^2. \end{aligned}$$

The fundamental theorem of symmetric polynomials plays an important role in the theory of algebraic equations. **Viéta** formulas can be obtained as follows. Let us consider the polynomial in $n+1$ variables

$$F(Y, X_1, \ldots, X_n) = (Y + X_1) \ldots (Y + X_n).$$

It is clear that

$$F(Y, X_1, \ldots, X_n) = Y^n + S_1 Y^{n-1} + \cdots + S_k Y^{n-k} + \cdots + S_n.$$

In particular, if a polynomial

$$f(X) = X^n + a_1 X^{n-1} + \cdots + a_{n-1} X + a_0 \tag{7.1}$$

has the roots $x_1, \ldots, x_n$, then it splits (over an algebraic closure) as

$$X^n + a_1 X^{n-1} + \cdots + a_{n-1} X + a_0 = (X - x_1) \ldots (X - x_n).$$

From the equality of polynomials

$$f(X) = (X - x_1)\dots(X - x_n) = X^n - S_1(x_1,\dots,x_n)X^{n-1} + \cdots + (-1)^k S_k(x_1,\dots,x_n)X^{n-k} + \cdots + (-1)^n S_n(x_1,\dots,x_n),$$

after identification of coefficients one obtains **Viéta** formulas:

$$\begin{aligned} a_1 &= -S_1(x_1,\dots,x_n) \\ &\dots \\ a_k &= (-1)^k S_k(x_1,\dots,x_n) \\ &\dots \\ a_n &= (-1)^n S_n(x_1,\dots,x_n). \end{aligned}$$

Their meaning is that every symmetric polynomial in the roots $x_1,\dots,x_n$ of the polynomial (7.1) can be expressed in terms of the coefficients $a_1,\dots,a_n$.

Now we present some applications of this important result.

Example 7.11 (Constructing a polynomial from its roots). *The polynomial $P(X) = aX^3 + bX^2 + cX + d$ $(d \neq 0)$ has the roots x_1, x_2, x_3. Find a polynomial whose roots are $1/x_1, 1/x_2, 1/x_3$.*

Solution. We compute Viète sums for the roots $1/x_1, 1/x_2, 1/x_3$ to get

$$\begin{aligned} \frac{1}{x_1} + \frac{1}{x_2} + \frac{1}{x_3} &= -c/d, \\ \frac{1}{x_1x_2} + \frac{1}{x_2x_3} + \frac{1}{x_3x_1} &= b/d, \\ \frac{1}{x_1x_2x_3} &= -a/d. \end{aligned}$$

Hence, such a polynomial is $X^3 + \frac{c}{d}X^2 + \frac{b}{d}X + \frac{a}{d}$. We can multiply it by d to obtain the polynomial $dX^3 + cX^2 + bX + a$. This is called the reciprocal polynomial of $aX^3 + bX^2 + cX + d$.

Alternatively, for the example above, one can assume that x is a root of $P(X)$, that is $ax^3 + bx^2 + cx + d = 0$. Since $d \neq 0$, we get $x \neq 0$. Then we can divide by x^3 and we obtain $a + b(1/x) + c(1/x)^2 + d(1/x)^3$. This shows that $1/x$ is a root of $dX^3 + cX^2 + bX + a$.

Definition 7.1. The polynomial $a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$ is called a **reciprocal polynomial** if its coefficients satisfy the relations:

$$a_n = a_0,\ a_{n-1} = a_1,\ a_{n-2} = a_2, \text{ and so on.}$$

Such a polynomial has the property that if x is a root, then $1/x$ is also a root. That is, its roots which are not ± 1 can be paired in to $\{x, 1/x\}$. Here is an application of this property.

Example 7.12 (Roots of a reciprocal polynomial). *Find the roots of the polynomial* $f(X) = 6X^4 + 5X^3 - 38X^2 + 5X + 6$.

Solution. This is a reciprocal polynomial, so we can denote its roots by $x, 1/x, y, 1/y$. Using Vieta relations we obtain the equalities:

$$x + y + \frac{1}{x} + \frac{1}{y} = -\frac{5}{6},$$
$$xy + \frac{x}{y} + \frac{y}{x} + \frac{1}{xy} + 2 = -\frac{19}{3}.$$

The second equality can be written as

$$\left(x + \frac{1}{x}\right)\left(y + \frac{1}{y}\right) = -\frac{25}{3}.$$

Denote $x + 1/x = u$ and $y + 1/y = v$. Then, from Vieta relations, we get the system: $u + v = -\frac{5}{6}$; $uv = -\frac{25}{3}$. Solving the system one obtains $u = \frac{5}{2}$ and $v = -\frac{10}{3}$. Solving the equations $x + \frac{1}{x} = \frac{5}{2}$ and $y + 1/y = -\frac{10}{3}$ one obtains the solutions $x_1 = 2$, $x_2 = -\frac{1}{2}$ and $y_1 = -3$, $y_2 = -\frac{1}{3}$. So, the roots of $f(X)$ are $2, -3, \frac{1}{2}, -\frac{1}{3}$.

Example 7.13. *Find the roots of the polynomial* $f(X) = X^4 + X^3 + X^2 + X + 1$.

Solution. This is a reciprocal polynomial. Let $z \in \mathbb{C}$ be a root. By the relation $z^4 + z^3 + z^2 + z + 1 = 0$, and because $z \neq 0$, we have

$$z^2 + z + 1 + \frac{1}{z} + \frac{1}{z^2} = 0.$$

By grouping the terms of the sum we obtain

$$\left(z + \frac{1}{z}\right)^2 + \left(z + \frac{1}{z}\right) - 1 = 0.$$

Let denote $z + 1/z = y$. Then y satisfies the equation $y^2 + y - 1 = 0$. Solving the quadratic equation one obtains $y_{1,2} = \frac{-1 \pm \sqrt{5}}{2}$. To find z we have to solve the quadratic equations:

$$z^2 + \frac{1 + \sqrt{5}}{2} z + 1 = 0,$$
$$z^2 + \frac{1 - \sqrt{5}}{2} z + 1 = 0.$$

After solving them one obtains the following four solutions

$$z_1 = \frac{\sqrt{5}-1}{4} + \frac{i}{2}\sqrt{\frac{5+\sqrt{5}}{2}};\ z_2 = \frac{\sqrt{5}-1}{4} - \frac{i}{2}\sqrt{\frac{5+\sqrt{5}}{2}}$$
$$z_3 = -\frac{\sqrt{5}+1}{4} + \frac{i}{2}\sqrt{\frac{5-\sqrt{5}}{2}};\ z_4 = -\frac{\sqrt{5}+1}{4} - \frac{i}{2}\sqrt{\frac{5-\sqrt{5}}{2}}.$$

We know that these roots are $z_k = \cos\frac{2k\pi}{5} + i\sin\frac{2k\pi}{5}$, where $k = 1,2,3,4$.

Identifying the quadrants we obtain, for example:

$$\cos\frac{2\pi}{5} = \frac{\sqrt{5}-1}{4} \text{ and } \sin\frac{2\pi}{5} = \sqrt{\frac{5+\sqrt{5}}{8}}$$

7.1.1 Newton's formulas

Let $P_k(x_1,\ldots,x_n) = x_1^k + x_2^k + \cdots + x_n^k$, $k = 0,1,\ldots$, be the sum of power k of the roots $x_1,x_2,\ldots,x_n$ of polynomial f. It is clear that P_k is a homogeneous symmetric polynomial of degree k in variables $x_1,x_2,\ldots,x_n$ hence, according to the fundamental theorem of symmetric polynomials, P_k can be expressed as a polynomial of $S_1,S_2,\ldots,S_n$, and finally in terms of the coefficients of polynomial. The problem to express P_k in terms of $S_1,S_2,\ldots,S_n$ is a difficult one. First of all we observe that for any $j \geq 0$ we have the recursive relation

$$P_{n+j} = -\frac{a_{n-1}}{a_n}P_{n+j-1} - \frac{a_{n-2}}{a_n}P_{n+j-2} - \cdots - \frac{a_1}{a_n}P_{j+1} - \frac{a_0}{a_n}P_j.$$

Hence, we can write successively $P_{n+1},P_{n+2},\ldots$ as linear combinations of $P_0,P_1,\ldots,P_{n-1}$, so the problem is reduced to expressing $P_0,P_1,\ldots,P_{n-1}$ in terms of $S_1,S_2,\ldots,S_n$. We need the following simple but important result.

Theorem 7.2. *Let f be a polynomial with roots $x_1,x_2,\ldots,x_n$. Then, for every value $x \neq x_1,x_2,\ldots,x_n$, the following relation holds:*

$$\frac{f'(x)}{f(x)} = \frac{1}{x-x_1} + \frac{1}{x-x_2} + \cdots + \frac{1}{x-x_n}.$$

Proof. One can write the polynomial function induced by f in the form $f(x) = a_n(x-x_1)(x-x_2)\cdots(x-x_n)$, then the derivative of f is

$$f'(x) = a_n\big[(x-x_2)\cdots(x-x_n) + (x-x_1)(x-x_3)\cdots(x-x_n) + \cdots + (x-x_1)(x-x_2)\cdots(x-x_{n-1})\big]$$

Replacing in $\frac{f'(x)}{f(x)}$ we get the desired formula. □

Now we can derive an algorithm in order to express $P_0, P_1, \ldots, P_{n-1}$ in terms of $S_1, S_2, \ldots, S_n$. From formula in Theorem 7.2 we have

$$f'(x) = \frac{f(x)}{x - x_1} + \frac{f(x)}{x - x_2} + \cdots + \frac{f(x)}{x - x_n}.$$

Dividing f by $x - x_k$ we get

$$\begin{aligned}\frac{f(x)}{x - x_k} = \frac{f(x) - f(x_k)}{x - x_k} &= a_n[x^{n-1} + (x_k - S_1)x^{n-2} + (x_k^2 - S_1 x_k + S_2)x^{n-3} \\ &+ \cdots + (x_k^{n-1} - S_1 x_k^{n-2} + S_2 x_k^{n-3} - \cdots - (-1)^{n-1} S_{n-1})].\end{aligned}$$

Summing for $k = 1, 2, \ldots, n$ it follows that

$$\begin{aligned}f'(x) = a_n\big[&nx^{n-1} + (P_1 - nS_1)x^{n-2} + (P_2 - S_1 P_1 + nS_2)x^{n-3} + \cdots \\ &+ (P_{n-1} - S_1 P_{n-2} + S_2 P_{n-3} - \cdots - (-1)^{n-1} n S_{n-1})\big].\end{aligned}$$

But according to Vieta's relations we have

$$f'(x) = a_n\left[x^{n-1} - (n-1)S_1 x^{n-2} + (n-2)S_2 x^{n-3} - \cdots\right].$$

Identifying coefficients in the above we get $P_1 - nS_1 = -(n-1)S_1$, then $P_2 - S_1 P_1 + nS_2 = (n-2)S_2$, and $P_3 - S_1 P_2 + S_2 P_1 - nS_3 = -(n-3)S_3$, ... Successively, these recover Newton's formulas

$$\begin{aligned} P_1 &= S_1 \\ P_2 - S_1 P_1 &= -2S_2 \\ P_3 - S_1 P_2 + S_2 P_1 &= 3S_3 \\ &\cdots \end{aligned}$$

which provide a way to express $P_0, P_1, \ldots, P_{n-1}$ in terms of $S_1, S_2, \ldots, S_n$:

$$\begin{aligned} P_0 &= n \\ P_1 &= S_1 \\ P_2 &= S_1^2 - 2S_2 \\ P_3 &= S_1^3 - 3S_1 S_2 + 3S_3 \\ &\cdots \end{aligned}$$

Here we extend the newton relations to powers sums P_k, where $k > 0$ can be even larger than the number of variables n.

In other words, for any n variables $X_1, \ldots, X_n$ and any $k > 0$, Newton formulas relate the polynomials $S_1, \ldots, S_n$ and $P_1, P_2, \ldots, P_k$ by the relations

$$P_k - S_1 P_{k-1} + S_2 P_{k-2} - \cdots + (-1)^{k-1} S_{k-1} P_1 + (-1)^k k S_k = 0. \tag{7.2}$$

There are many proofs of Newton's identities. One using calculus and the logarithmic derivative can be found in [106], while a combinatorial proof is given in [266]. Here we present a simple, purely algebraic proof.

Let $x_1,\ldots,x_n \in \mathbb{C}$ be arbitrary complex numbers. It is enough to show that the equality (7.2) when we evaluate the polynomials in $x_1,\ldots,x_n$. We start by first proving the case $k=n$ and then we will derive the general formulas.

Suppose $f \in \mathbb{C}[X]$ is a monic polynomial with roots $x_1,\ldots,x_n$. Recall that

$$f(X) = X^n + \sum_{i=1}^{n} (-1)^i S_i(x_1,\ldots,x_n) X^{n-i}.$$

Evaluating f at x_j for $j = 1,2,\ldots,n$ we get

$$x_j^n + \sum_{i=1}^{n} (-1)^i S_i(x_1,\ldots,x_n) x_j^{n-i} = 0.$$

Summing over all $j = 1,\ldots,n$, and using $P_0 = n$ we obtain that

$$P_n(x_1,\ldots,x_n) + \sum_{i=1}^{n} (-1)^i S_i(x_1,\ldots,x_n) P_{n-i}(x_1,\ldots,x_n) = 0.$$

As this is true for any $x_1,\ldots,x_n \in \mathbb{C}$, we get that (7.2) holds in the particular case $n=k$. Suppose now that $k > n$ and let $x_1,x_2,\ldots,x_n,x_{n+1},\ldots,x_k \in \mathbb{C}$ be arbitrary. Consider $f \in \mathbb{C}[X]$ the monic polinomial having roots $x_1,\ldots,x_n$ and $g \in \mathbb{C}[X]$ the monic polynomial with roots $x_1,x_2,\ldots,x_k$. More precisely,

$$g(X) = f(X) \cdot \prod_{i=n+1}^{k} (X - x_i).$$

We run now apply the previous argument for symmetric sums in k variables to the polynomial g and then set $x_{n+1} = x_{n+2} = \cdots = x_k = 0$.

The desired identity (7.2) follows, since for every $i \in \{1,2,\ldots,k\}$ we have

$$S_i(x_1,\ldots,x_k) = \sum_{j_1<j_2<\cdots<j_i} x_{j_1} x_{j_2} \ldots x_{j_i},$$

any term in which x_j appears for $j > n$ becomes 0.

We just need to justify formula (7.2) when $k < n$. Consider the polynomial

$$F(X_1,\ldots,X_n) = P_k - S_1 P_{k-1} + S_2 P_{k-2} - \cdots + (-1)^{k-1} S_{k-1} P_1 + (-1)^k k S_k.$$

As F is a homogeneous polynomial of degree k, it can be written as

$$F(X_1,\ldots,X_n) = \sum_{a_1,a_2,\ldots,a_n} c(a_1,a_2,\ldots,a_n) X_1^{a_1} X_2^{a_2} \ldots X_n^{a_n},$$

where $a_1, \ldots, a_n$ are non-negative integers such that $a_1 + a_2 + \cdots + a_n = k$.

Each monomial in F does not contain more than k variables. Fix one monomial $c(a_1, a_2, \ldots, a_n) X_1^{a_1} X_2^{a_2} \ldots X_n^{a_n}$. By substituting 0 for $n - k$ variables in F, we can make sure that the monomial $c(a_1, a_2, \ldots, a_n) X_1^{a_1} X_2^{a_2} \ldots X_n^{a_n}$ survives. But the same monomial can be found in the polynomial arising from a version of Newton's identities for k variables, therefore it must be 0. We can repeat the procedure, i.e. substituting 0 for (possibly other) $n - k$ variables to show that the polynomial F is identically zero. This concludes the proof of the Newton's identities.

By fixing the fundamental symmetric polynomials S_i, the Newton identities (7.2) can be regarded as linear equations in the unknowns P_j and one can use linear algebra to express

$$P_k = \begin{vmatrix} S_1 & 1 & 0 & \ldots & 0 \\ 2S_2 & S_1 & 1 & \ldots & 0 \\ 3S_3 & S_2 & S_1 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ kS_k & S_{k-1} & S_{k-2} & \ldots & S_1 \end{vmatrix}, \text{ for any } k \in \mathbb{N}^*. \tag{7.3}$$

Similarly, by fixing the P_j, one can find S_i in terms of P_j as follows

$$S_k = \frac{1}{k!} \begin{vmatrix} P_1 & 1 & 0 & \ldots & 0 & 0 \\ P_2 & P_1 & 2 & \ldots & 0 & \\ P_3 & P_2 & P_1 & \ldots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \\ P_{k-1} & P_{k-2} & P_{k-3} & \ldots & P_1 & k-1 \\ P_k & P_{k-1} & P_{k-2} & \ldots & P_2 & P_1 \end{vmatrix}, \text{ for any } k \in \mathbb{N}^*. \tag{7.4}$$

The following result gives an explicit formula for the symmetric polynomials S_k in terms of the symmetric power sums P_j, $j = 0, 1, 2, \ldots$

Theorem 7.3. *The following formula holds*

$$S_k = (-1)^k \sum_{l_1 + 2l_2 + \ldots + kl_k = k} (-1)^{l_1 + \ldots + l_k} \frac{P_1^{l_1}}{1^{l_1} l_1!} \frac{P_2^{l_2}}{2^{l_2} l_2!} \cdots \frac{P_k^{l_k}}{k^{l_k} l_k!}. \tag{7.5}$$

Proof. Suppose $x_1, x_2, \ldots, x_n$ are the variables of the polynomials $S_1, \ldots, S_n$. Adding an extra variable z, we observe the following identities of formal power series in z:

$$\sum_{k=0}^{n}(-1)^k S_k z^k = \prod_{j=1}^{n}(1-x_j z^j) = e^{\sum_{j=1}^{n}\ln(1-x_j z^j)} = e^{-\sum\limits_{j=1}^{n}\sum\limits_{m=1}^{\infty}\frac{x_j^m z^m}{m}}$$

$$= e^{-\sum\limits_{s=1}^{\infty}\frac{P_s z^s}{s}} = \prod_{s=1}^{\infty} e^{-\frac{P_s z^s}{s}} = \prod_{s=1}^{\infty}\sum_{t=0}^{\infty}\frac{1}{t!}\left(-\frac{P_s z^s}{s}\right)^t$$

$$= \sum_{k=0}^{\infty}\left(\sum_{l_1+2l_2+\ldots=k}\frac{\left(-\frac{P_1}{1}\right)^{l_1}}{l_1!}\cdot\frac{\left(-\frac{P_2}{2}\right)^{l_2}}{l_2!}\cdots\right)z^k$$

$$= \sum_{k=0}^{\infty}\left(\sum_{l_1+2l_2+\ldots+kl_k=k}(-1)^{l_1+\ldots+l_k}\frac{P_1^{l_1}}{1^{l_1}l_1!}\frac{P_2^{l_2}}{2^{l_2}l_2!}\cdots\frac{P_k^{l_k}}{k^{l_k}l_k!}\right)z^k.$$

The conclusion follows by identifying the coefficients of z^k. □

Remark. By the theorem above it follows that for every $k \geq n+1$ we have

$$\sum_{l_1+2l_2+\ldots+kl_k=k}(-1)^{l_1+\ldots+l_k}\frac{P_1^{l_1}}{1^{l_1}l_1!}\frac{P_2^{l_2}}{2^{l_2}l_2!}\cdots\frac{P_k^{l_k}}{k^{l_k}l_k!} = 0.$$

Remark. In the proof above, we note that the Diophantine equation

$$x_1 + 2x_2 + \ldots + kx_k = k,$$

plays a fundamental role. For fixed $k \geq 1$, note that the number of non-negative solutions $(x_1, x_2, \ldots, x_k) \in \mathbb{N}^k$ for this equation is exactly $p(k)$, the number of partitions of k. Note that $p(1) = 1$, $p(2) = 2$, $p(3) = 3$. For $k = 4$, the only solutions are given by $(0,0,0,1)$, $(1,0,1,0)$, $(0,2,0,0)$, $(2,1,0,0)$, $(4,0,0,0)$, so $p(4) = 5$. In general, the number of solutions $p(k)$ is encoded as the coefficient of $p(k)$ in the formal power-series expansion of

$$f_k(z) = \prod_{j=1}^{k}\sum_{m=1}^{\infty}(1 + z^j + z^{2j} + \cdots) = \prod_{j=1}^{k}\frac{1}{1-z^j} \text{ for all } z \text{ such that } |z| < 1.$$

It is easy to deduce now that for every $k \geq 2$,

$$p(k) = \frac{1}{k!}f_k^{(k)}(0), \tag{7.6}$$

where $f_k^{(k)}$ denotes the k-th derivative of f. Indeed, one could verify that this formula gives $p(4) = 5$ and $p(5) = 7$. However, the formula (7.6) becomes too complicated to compute the number of partitions $p(k)$ for high values of k. It is known that the partition function $p(k)$ is notoriously complicated and no closed form formula for this function is known.

The sequence $p(k)$ is indexed as A000041 in the OEIS [211], and starts with the following terms

$$1,1,2,3,5,7,11,15,22,30,42,56,77,101,135,176,231,297,385,490,627,792,\ldots.$$

An asymptotic formula was first discovered by Hardy and Ramanujan and later improved by Rademacher. This asserts that

$$p(k) \sim \frac{1}{4k\sqrt{3}} e^{\pi\sqrt{2k/3}}, \text{ as } k \to \infty. \tag{7.7}$$

The theory of modular forms can be applied to reveal some intriguing arithmetic properties carried by the partition function $p(k)$. An example of this is that $p(5k+4) \equiv 0 \pmod 5$ for all $k \in \mathbb{N}$. There is an extremely rich literature on the subject of partitions. One of the standard references for connections of $p(k)$ with number theory is the book by Andrews [12].

Example 7.14 (Asian-Pacific 2003). *If the roots of the polynomial*

$$P(x) = x^8 - 4x^7 + 7x^6 + a_5x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$$

are all positive real numbers, find all possible values of a_0.

Solution. Let the roots be $r_1, r_2, \ldots, r_8$. By Vieta's formulas, we have

$$S_1 = r_1 + r_2 + \cdots + r_8 = 4 \text{ and } e_2 = 7.$$

The value of S_2 does not seem particularly helpful in the form in which it is given, so we recall that Newton's identities give

$$a_8P_2 + a_7P_1 + 2a_6 = 0, \quad P_2 + (-4)(4) + 2(7) = 0,$$

so $P_2 = r_1^2 + r_2^2 + \cdots + r_8^2 = 2$. It seems that we have run into another dead end here, unless we recall the well-known Cauchy-Schwarz Inequality, which states that, for real numbers $x_1, x_2, \ldots, x_n$ and $y_1, y_2, \ldots, y_n$, we have

$$(x_1y_1 + x_2y_2 + \cdots + x_ny_n)^2 \le \left(x_1^2 + x_2^2 + \cdots + x_n^2\right)\left(y_1^2 + y_2^2 + \cdots + y_n^2\right),$$

with equality if and only if $x_1/y_1 = x_2/y_2 = \ldots = x_8/y_8$. In this case, we put $x_1 = x_2 = \ldots = x_8 = 1$ and $y_i = r_i$ to get

$$(r_1 + r_2 + \cdots + r_n)^2 \le 8\left(r_1^2 + r_2^2 + \cdots + r_8^2\right).$$

Since equality holds, we must have $r_1 = r_2 = \ldots = r_8 = 1/2$, and thus

$$a_0 = r_1r_2\cdots r_8 = \frac{1}{256}.$$

Example 7.15. *Find all solutions, real or complex, to the system of equations*

$$\begin{cases} x+y+z=3 \\ x^2+y^2+z^2=3 \\ x^3+y^3+z^3=3. \end{cases}$$

Solution. Assume without loss of generality that x,y,z are the roots of a cubic polynomial with leading coefficient 1. Since $S_1=3$, we find $a_2=-3$. Hence, we know that the polynomial has the form

$$f(r)=r^3-3r^2+a_1r+a_0.$$

By Newton's sums, we have

$$\begin{aligned} a_3P_2+a_2P_1+2a_1&=0,\\ (1)(3)+(-3)(3)+2a_1&=0,\\ a_1&=3,\\ a_3P_3+a_2P_2+a_1P_1+3a_0&=0,\\ (1)(3)+(-3)(3)+(3)(3)+3a_0&=0,\\ a_0&=-1. \end{aligned}$$

Thus $f(r)=r^3-3r^2+3r-1=(r-1)^3$, so the only solution is $x=y=z=1$.

Example 7.16. *Let x_1,x_2,x_3 be the roots of $x^3-x+1=0$. Find $x_1^{10}+x_2^{10}+x_3^{10}$.*

Solution. Recall the notation $P_k=x_1^k+x_2^k+x_3^k$, $k=0,1,\ldots$. We have $a_1=0$, $a_2=-1$, $a_3=-1$, and from Newton's formulas we get

$$P_{k+3}=P_{k+1}-P_k,\quad k=0,1,\ldots.$$

It is clear that $P_0=3$, $P_1=0$, $P_2=2$. Then, applying successively the above recursion relation, one obtains

$$\begin{aligned} P_3&=P_1-P_0=-3,\\ P_4&=P_2-P_1=2,\\ P_5&=P_3-P_2=-5,\\ P_6&=P_4-P_3=5,\\ P_7&=P_5-P_4=-7,\\ P_8&=P_6-P_5=10,\\ P_9&=P_7-P_6=-12,\\ P_{10}&=P_8-P_7=17, \end{aligned}$$

which is the quantity we are asked for.

Example 7.17. *Find all the values of $a \in \mathbb{R}$ such that the zeros x_1, x_2, x_3 of the polynomial $x^3 - 6x^2 + ax + a$ satisfy*

$$(x_1 - 3)^3 + (x_2 - 3)^3 + (x_3 - 3)^3 = 0.$$

Solution. We use Newton's formulas for $P_k = x_1^k + x_2^k + x_3^k$, $k = 2,3$. Since x_1, x_2, x_3 are zeros of the given polynomial, we have $S_1 = 6$, $S_2 = a$, $S_3 = -a$, and therefore

$$\begin{aligned} P_1 &= S_1 = 6, \\ P_2 &= S_1^2 - 2S_2 = 36 - 2a, \\ P_3 &= S_1^3 - 3S_1S_2 + 3S_3 = 216 - 21a. \end{aligned}$$

Using the binomial theorem we then obtain

$$\begin{aligned} 0 &= (x_1 - 3)^3 + (x_2 - 3)^3 + (x_3 - 3)^3 = s_3 - 3s_2 \cdot 3 + 3s_1 \cdot 3^2 - 3 \cdot 3^3 \\ &= 216 - 21a - 9(36 - 2a) + 27 \cdot 6 - 81 = -27 - 3a, \end{aligned}$$

and therefore $a = -9$.

Example 7.18 (IMO 1985). *Let a, b, c, d be real numbers such that*

$$a + b + c + d = a^7 + b^7 + c^7 + d^7 = 0.$$

Show that $a(a + b)(a + c)(a + d) = 0$.

Solution. We use the notation $P_k(a,b,c,d) = a^k + b^k + c^k + d^k$ for the Newton sums and $S_k = S_k(a,b,c,d)$ for the elementary symmetric polynomials in a, b, c, d, $k = 1, 2, \ldots$. We have $P_1 = S_1 = 0$. From Newton's formulas we get successively:

$$\begin{aligned} &P_2 = S_1P_1 - 2S_2, \text{ hence } P_2 = -2S_2, \\ &P_3 = S_1P_2 - S_2P_1 + 3S_3, \text{ hence } P_3 = 3S_3, \\ &P_4 = S_1P_3 - S_2P_2 + S_3P_1 - 4S_4, \text{ hence } P_4 = 2S_2^2 - 4S_4, \\ &P_5 = S_1P_4 - S_2P_3 + S_3P_2 - S_4P_1, \text{ hence } P_5 = -5S_2S_3, \\ &P_6 = S_1P_5 - S_2P_4 + S_3P_3 - S_4P_2, \text{ hence } P_6 = -2S_2^4 + 6S_2S_4 + 3S_3^2, \\ &P_7 = S_1P_6 - S_2P_5 + S_3P_4 - S_4P_3, \text{ hence } P_7 = S_3(7S_2^2 - 5S_4). \end{aligned}$$

Because $P_7 = 0$, it follows that $S_3(7S_2^2 - 5S_4) = 0$.

There are two cases: $S_3 = 0$ or $7S_2^2 - 5S_4 = 0$. We have to prove that

$$a\left[a^3 + a^2(b + c + d) + a(bc + cd + db) + bcd\right] = 0.$$

This is equivalent to

$$a^3(a+b+c+d) = -aS_3,$$

and $S_3 = 0$ gives the result.

Assume that $7S_2^2 - 5S_4 = 0$, that is $S_2^2 = \frac{5}{7}S_4$. From $P_4 = 2S_2^2 - 4S_4 \geq 0$, we have $S_2^2 \geq 2S_4$, which is in contradiction with $S_2^2 = \frac{5}{7}S_4$.

Example 7.19. *Let the roots of $x^3 + 2x^2 + 3x + 4 = 0$ be a, b, c. Find $a^2 + b^2 + c^2$.*
Solution. Recall that

$$(a+b+c)^2 = a^2 + b^2 + c^2 + 2(ab + bc + ca).$$

Then, we get

$$a^2 + b^2 + c^2 = (a+b+c)^2 - 2(ab + bc + ca).$$

By Viete's formulas, $a + b + c = -2$ and $ab + bc + ca = 3$, so that

$$a^2 + b^2 + c^2 = -2.$$

Remark. According to Newton's identities we have

$$P_2 = a_1P_1 - 2a_2 = a_1^2 - 2a_2 = 4 - 2 \cdot 3 = -2.$$

Example 7.20. *Find the sum of the fourth powers of the roots of the equation*

$$7x^3 - 21x^2 + 9x + 2 = 0.$$

Solution. First we write the equation as

$$x^3 - 3x^2 + \frac{9}{7}x + \frac{2}{7} = 0.$$

We have $a_1 = 3$, $a_2 = \frac{9}{7}$, $a_3 = -\frac{2}{7}$, $a_4 = 0$, and by Newton's identities we get

$$\begin{aligned}
&P_1 = 3,\\
&P_2 = 3P_1 - 2a_2 = 9 - \frac{18}{7} = \frac{45}{7},\\
&P_3 = a_1P_2 - a_2P_1 + 3a_3 = 3 \cdot \frac{45}{7} - \frac{9}{7} \cdot 3 - \frac{6}{7} = \frac{102}{7},\\
&P_4 = a_1P_3 - a_2P_2 + a_3P_1 - 4a_4 = 3 \cdot \frac{102}{7} - \frac{9}{7} \cdot \frac{45}{7} - \frac{6}{7} = \frac{1695}{49}.
\end{aligned}$$

Example 7.21 (AIME 2003). *The roots of $x^4 - x^3 - x^2 - 1 = 0$ are a, b, c, and d. Find $p(a) + p(b) + p(c) + p(d)$, where*

$$p(x) = x^6 - x^5 - x^3 - x^2 - x.$$

Solution. We have

$$\begin{aligned} p(a) &= a^6 - a^5 - a^3 - a^2 - a = a^6 - a^5 - a^4 - a^2 + a^4 - a^3 - a \\ &= a^2(a^4 - a^3 - a^2 - 1) + (a^4 - a^3 - a^2 - 1) + a^2 - a + 1 = a^2 - a + 1, \end{aligned}$$

and similarly

$$p(b) = b^2 - b + 1, \quad p(c) = c^2 - c + 1, \quad p(d) = d^2 - d + 1.$$

It follows that

$$p(a) + p(b) + p(c) + p(d) = \sum a^2 - \sum a + 4.$$

From Newton's identities we get

$$P_2 = a_1 P_1 - 2a_2 = a_1^2 - 2a_2 = 1 + 2 = 3,$$

hence

$$p(a) + p(b) + p(c) + p(d) = 3 - 1 + 4 = 6.$$

Example 7.22. *Let $x_1, x_2, \ldots, x_n$ and $y_1, y_2, \ldots, y_n$ complex numbers such that*

$$x_1^k + x_2^k + \cdots + x_n^k = y_1^k + y_2^k + \cdots + y_n^k, \quad k = 1, 2, \ldots, n.$$

Show that $x_1, x_2, \ldots, x_n$ and $y_1, y_2, \ldots, y_n$ are the same, up to ordering.

Solution. Denote $a_k = S_k(x_1, \ldots, x_n)$ and $b_k = S_k(y_1, \ldots, y_n)$. Using Newton formulas for the two series of numbers, we see that $a_k = b_k$ for all $k = 1, \ldots, n$. Hence, the numbers $x_1, x_2, \ldots, x_n$ and $y_1, y_2, \ldots, y_n$ are the roots of the same algebraic equation of degree n.

Example 7.23. *Let $x_1, x_2, \ldots, x_n$ be complex numbers. Show that if the Newton sums $P_1(x_1, \ldots, x_n) = P_2(x_1, \ldots, x_n) = \cdots = P_{n+1}(x_1, \ldots, x_n)$ then $x_i \in \{0, 1\}$ for all i. Prove that if $x_1, x_2, \ldots, x_n$ are real numbers then the above hypothesis can be replaced by $P_2 = P_3 = P_4$.*

Solution. First, we remark that $S_i(X_1, \ldots, X_k, 0, \ldots, 0) = S_i(X_1, \ldots, X_k)$, for all $1 \leq i \leq n$ and all $1 \leq k \leq n$. Therefore, the hypothesis do not change if we assume that all numbers are non zero. Denote by $S_i = S_i(x_1, \ldots, x_n)$. By the Newton formulas we have the equality:

$$P_{n+1} - S_1 P_n + S_2 P_{n-1} + \cdots + (-1)^n S_n P_1 = 0.$$

Using the equality $P_1 = P_2 = \cdots = P_{n+1}$ we obtain the identity

$$1 - S_1 + S_2 - \cdots + (-1)nS_n = 0,$$

which gives

$$(1 - x_1)(1 - x_2)\cdots(1 - x_n) = 0.$$

Assume that $x_n = 1$. The hypothesis reproduces for the numbers $x_1, \ldots, x_{n-1}$ and then, use induction.
In the case of real numbers, $P_2 = P_3 = P_4$ implies that $P_2 - 2P_3 + P_4 = 0$, which can be written

$$\sum_{i=1}^{n} x_i^2 (1 - x_i)^2 = 0.$$

The conclusion is now obvious.

Example 7.24. *Let a, b, c and d be real numbers such that $a + b + c + d = 0$ and $a^7 + b^7 + c^7 + d^7 = 0$. Show that $(a + b)(a + c)(a + d) = 0$.*

Solution. Apply Newton formulas to compute P_1 to P_7. One obtains the equalities $P_2 = -2S_2$, $P_3 = S_3$, $P_4 = 2S_2^2 - 4S_4$, $P_5 = -5S_2S_3$ and, finally, from $P_7 = 0$ one has $7S_3(S_4 - S_2^2) = 0$.

If $S_4 - S_2^2 = 0$, one obtains $P_4 = -2S_2^2$, which means that $a = b = c = d = 0$.

In the case $S_3 = 0$ one can see, using $P_1 = 0$, that this is equivalent to

$$(a + b)(a + c)(a + d) = 0.$$

Example 7.25. *Let p be a prime number. Find $1^k + 2^k + \cdots + (p - 1)^k \pmod{p}$.*

Solution. The classes $1, 2, \ldots, p - 1$ are the roots of the polynomial $X^{p-1} - 1$. Using Viète formulas and then Newton formulas we get $P_1 = \cdots = P_{p-2} = 0$ and $P_{p-1} = -1$.

7.2 Number theoretic applications of symmetric polynomials

Given a polynomial $f \in \mathbb{C}[X]$, can one decide if it has a double zero only by performing additions, multiplications and divisions on its coefficients? The answer to this question is yes. Let $x_1, \ldots, x_n$ be the roots of f counted with multiplicity. Then, f has a double root if and only if $F(x_1, \ldots, x_n) = 0$, where

$$F(x_1, \ldots, x_n) = \prod_{1 \le i < j \le n} (x_i - x_j)^2.$$

Clearly, F is a symmetric polynomial in $x_1,\dots,x_n$, hence by the fundamental theorem of symmetric polynomials, F can be written as a polynomial expression in the symmetric sums $S_1(x_1,\dots,x_n),\dots,S_n(x_1,\dots,x_n)$.

Using Vieta's relations, the symmetric sums are equal to the coefficients of f, up to sign. Therefore, deciding whether $F(x_1,\dots,x_n)=0$ amounts to performing operations such as additions, multiplications and divisions on the coefficients of f. Notice that the only divisions one might have to perform are divisions by the dominant coefficient of f.

Let us bring our attention to one of the challenge problems from the previous set, which we now give as a Lemma.

Lemma 7.1. *Let $f\in\mathbb{Q}[X_1,\dots,X_n]$ be a symmetric polynomial and $g(X)\in\mathbb{Q}[X]$ be a polynomial of degree n having $z_1,\dots,z_n\in\mathbb{C}$ as roots. Then $f(z_1,\dots,z_n)\in\mathbb{Q}$. Moreover, if g is monic, then the conclusion still holds if we replace $\mathbb{Q}$ with $\mathbb{Z}$ in every instance of this lemma.*

Proof. Using the fundamental theorem of symmetric polynomials one can write $f(z_1,\dots,z_n)$ as a polynomial $h(S_1(z_1,\dots,z_n),\dots,S_n(z_1,\dots,z_n))$. Now $S_i(z_1,\dots,z_n)$ are rational numbers, as the coefficients of g are rational. The case when g is monic with integer coefficients follows by the same proof. □

Let us now have a look at the following corollary.

Corollary 7.1. *Let $f\in\mathbb{Z}[X]$ be a monic polynomial of degree n with complex roots $z_1,\dots,z_n\in\mathbb{C}$. Then for any prime p, $(z_1+z_2+\cdots+z_n)^p-(z_1^p+\cdots+z_n^p)\in\mathbb{Z}$. Moreover, one has*

$$p\mid(z_1+z_2+\cdots+z_n)^p-\left(z_1^p+\cdots+z_n^p\right).$$

Proof. The previous lemma implies immediately that

$$z_1^p+z_2^p+\cdots+z_n^p\in\mathbb{Z}\text{ and }(z_1+z_2+\cdots+z_n)^p\in\mathbb{Z}.$$

Consider now

$$q(X_1,\dots,X_n)=\frac{X_1^p+\cdots+X_n^p-(X_1+\cdots+X_n)^p}{p}\in\mathbb{Q}[X_1,\dots,X_n].$$

Using the multinomial formula it is easy to see that in fact all coefficients of q are integers. Hence $q(z_1,\dots,z_n)\in\mathbb{Z}$, by the previous Lemma. □

7.2.1 Algebraic numbers and algebraic integers

Definition 7.2. A number $z\in\mathbb{C}$ is **algebraic** if there is a non-zero $f\in\mathbb{Q}[X]$ with $f(z)=0$. For an algebraic number z, its minimal polynomial $m_z\in\mathbb{Q}[X]$ is the monic polynomial of smallest degree which has z as a root.

One many notice that the minimal polynomial m_z of an algebraic number z is unique and irreducible in $\mathbb{Q}[X]$. Moreover, if $f \in \mathbb{Q}[X]$ is such that $f(z) = 0$, then $m_z \mid f$ in $\mathbb{Q}[X]$. The roots of m_z are called the "conjugates" of z.

Definition 7.3. A number $z \in \mathbb{C}$ is an **algebraic integer** if there exists a monic $f \in \mathbb{Z}[X]$ such that $f(z) = 0$. Algebraic integers are exactly the algebraic numbers for which $m_z \in \mathbb{Z}[X]$.

The set of algebraic numbers is denoted by $\overline{\mathbb{Q}}$ and the set of algebraic integers by $\overline{\mathbb{Z}}$. We next show that the sum and product of two algebraic numbers (or algebraic integers) is an algebraic number (or algebraic integer).

Theorem 7.4. *The sets $\overline{\mathbb{Z}}$ and $\overline{\mathbb{Q}}$ are subrings of $\mathbb{C}$.*

Proof. Let $\alpha, \beta \in \overline{\mathbb{Q}}$ and denote by $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_n$ and by $\beta_1 = \beta, \beta_2, \ldots, \beta_m$ are the conjugates of α and β, respectively. Recall that the α_i's and β_j's are the roots of some irreducible polynomials with coefficients in $\mathbb{Q}$. Consider

$$f(X) = \prod_{i=1}^{n}\prod_{j=1}^{m}(X - \alpha_i - \beta_j) \in \mathbb{C}[X].$$

We first claim that f has rational coefficients. As $\alpha + \beta$ is a root of f, so this would prove that $\alpha + \beta \in \overline{\mathbb{Q}}$.

To prove the claim, let us focus on a coefficient of f. This is a polynomial expression in α_i, β_j. It is invariant under permutations of $\alpha_1, \ldots, \alpha_n$ and also under permutations of $\beta_1, \ldots, \beta_m$. Let us see this coefficient c as a polynomial with coefficients in the ring $\mathbb{Q}[\beta_1, \ldots, \beta_m]$ which is symmetric in $\alpha_1, \ldots, \alpha_n$.

By the fundamental theorem of symmetric polynomials we have

$$c(\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_m) = B(S_1(\alpha_1, \ldots, \alpha_n), \ldots, S_n(\alpha_1, \ldots, \alpha_n)),$$

where $B \in (\mathbb{Q}[\beta_1, \ldots, \beta_m])[X_1, \ldots, X_n]$. Each of the n entries of this polynomial is a rational number, so

$$c(\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_m) \in \mathbb{Q}[\beta_1, \ldots, \beta_m].$$

But c is symmetric in $\beta_1, \ldots, \beta_m$, hence

$$c(\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_m) = B'(S_1(\beta_1, \ldots, \beta_m), \ldots, S_m(\beta_1, \ldots, \beta_m)),$$

where $B' \in \mathbb{Q}[X_1, \ldots, X_m]$. Again, each entry in the evaluation of the polynomial B' is a rational number, hence c is rational, proving that $\alpha + \beta \in \overline{\mathbb{Q}}$.

To show that $\alpha\beta \in \overline{\mathbb{Q}}$ one can apply the same strategy for the polynomial

$$g(X) = \prod_{i=1}^{n}\prod_{j=1}^{m}(X - \alpha_i\beta_j).$$

The proof for algebraic integers is obtained by replacing $\mathbb{Q}$ with $\mathbb{Z}$. □

Note that $\overline{\mathbb{Q}}$ is in fact a field. Indeed, let $z \in \overline{\mathbb{Q}} \setminus \{0\}$. Then, its minimal polynomial $m_z(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$ has $a_0 \neq 0$, hence

$$z^n + a_{n-1}z^{n-1} + \cdots + a_1z + a_0 = 0,$$

from where

$$1 + a_{n-1}\left(\frac{1}{z}\right) + \cdots + \left(\frac{1}{z}\right)^n = 0,$$

hence z^{-1} is an algebraic number.

The example we are about to discuss generated a whole mathematical theory and was probably the source of an important area of research in transcendental number theory. Let us start by introducing a definition.

Definition 7.4. For a polynomial $f(X) = a_n(X - x_1)\ldots(X - x_n) \in \mathbb{C}[X]$, we define its **Mahler measure** to be

$$M(f) = |a_n| \max(1, |x_1|) \cdot \cdots \cdot \max(1, |x_n|).$$

It is easy to see that $M(f \cdot g) = M(f) \cdot M(g)$, for all $f, g \in \mathbb{C}[X]$. Using complex analysis one can prove that

$$M(f) = e^{\int_0^1 \ln|f(e^{2i\pi t})|}.$$

We now present the following beautiful result of Kronecker.

Theorem 7.5. *Let $f \in \mathbb{Z}[X]$ be a monic polynomial with $f(0) \neq 0$ and $M(f) = 1$. Then, for all $z \in \mathbb{C}$ such that $f(z) = 0$, there exists $n \in \mathbb{N}$ such that $z^n = 1$.*

Proof. Let $x_1, \ldots, x_n \in \overline{\mathbb{Q}} \subseteq \mathbb{C}$ be the roots of f, counted with multiplicity. Consider the polynomials

$$f_k(X) = \left(X - x_1^k\right) \cdot \cdots \cdot \left(X - x_n^k\right).$$

The coefficients of these polynomials are symmetric polynomial expressions in $x_1, \ldots, x_k$, hence $f_k \in \mathbb{Z}[X]$. Moreover, note that the coefficients of f_k are bounded above by $\binom{n}{\lfloor \frac{n}{2} \rfloor}$. This implies that there are only finitely many polynomials f_k, so there are $i, j \in \mathbb{N}$, with $i > j$ such that $f_i = f_j$.

The latter equality in $\mathbb{Z}[X]$ gives

$$\left(X - x_1^i\right) \cdots \left(X - x_n^i\right) = \left(X - x_1^j\right) \cdots \left(X - x_n^j\right).$$

We deduce that there exists a permutation $\sigma \in S_n$ such that

$$x_1^i = x_{\sigma(1)}^j, \ldots, x_n^i = x_{\sigma(n)}^j.$$

Let us now focus on the first zero x_1. Remark that

$$x_1^{i^2} = (x_1^i)^i = \left(x_{\sigma(1)}^j\right)^i = \left(x_{\sigma(1)}^i\right)^j = x_{\sigma(\sigma(1))}^{j^2}.$$

Inductively, we get $x_1^{i^r} = x_{\sigma^r(1)}^{j^r}$ for any $r \in \mathbb{N}$, where σ^r is the permutation obtained by composing σ with itself r times.

As the order of the group S_n is $n!$, we have that

$$x_1^{i^{n!}} = x_1^{j^{n!}},$$

so $x_1^{i^{n!}-j^{n!}} = 1$ and this shows that x_1 is an $i^{n!} - j^{n!}$ root of unity. □

We end this section with a question: are there algebraic integers lying on the unit circle which are not roots of unity?

Example 7.26. *Consider the sequence $(x_n)_{n\geq 0}$ defined by $x_0 = 4$, $x_1 = x_2 = 0$, $x_3 = 3$ and $x_{n+4} = x_{n+1} + x_n$. Prove that for any prime p, x_p is a multiple of p.*

Solution. The characteristic polynomial of the recursive relation is given by $f(X) = X^4 - X - 1$. It is easy to see that f cannot have a double zero (by looking at the derivative f', for instance).

Using the theory of linear recursive sequences, it follows that the general term of the sequence is of the form $Ar_1^n + Br_2^n + Cr_3^n + Dr_4^n$ for some constants A, B, C, D. Here r_i are the distinct zeros of the characteristic polynomial. Because this polynomial has no rational zero, it is natural to suppose that $Ar_1^n + Br_2^n + Cr_3^n + Dr_4^n$ is symmetric in r_1, r_2, r_3 and r_4. Thus, $A = B = C = D$. This result can also be proved rigorously using Galois theory, but such a proof goes beyond the scope of this book.

We will prove that $x_n = r_1^n + r_2^n + r_3^n + r_4^n$ using induction on n. For $n \leq 4$, the assertion follows from Viete's formulae. To prove that it holds for any n, just notice that $r_i^{n+4} = r_i^{n+1} + r_i^n$. The induction can be completed easily. We are left to prove that p divides $r_1^p + r_2^p + r_3^p + r_4^p$ for any prime number p. This follows from Corollary 7.1.

Example 7.27. *Let $a_1, a_2, \ldots, a_k$ be positive real numbers such that*

$$\sqrt[n]{a_1} + \sqrt[n]{a_2} + \cdots + \sqrt[n]{a_k}$$

is a rational number for all $n \geq 2$. Prove that $a_1 = a_2 = \cdots = a_k = 1$.

Solution. First, we will prove that $a_1, a_2, \ldots, a_k$ are algebraic numbers and that $a_1 a_2 \cdots a_k = 1$. Take an integer $N > k$ and set

$$x_1 = \sqrt[N!]{a_1}, \quad x_2 = \sqrt[n!]{a_2}, \quad \ldots, \quad x_k = \sqrt[n!]{a_k}.$$

Then clearly $x_1^j + x_2^j + \cdots + x_k^j$ is rational for all $1 \leq j \leq N$.

Using Newton's formulae, we can easily deduce that all the symmetric fundamental sums of $x_1, x_2, \ldots, x_k$ are rational numbers. Hence $x_1, x_2, \ldots, x_k$ are algebraic numbers and so are $a_1, a_2, \ldots, a_k$. As we previously mentioned, from the Newton's formula we deduced that

$$x_1 \cdot x_2 \cdot \cdots \cdot x_k = \sqrt[n!]{a_1 a_2 \ldots a_k}$$

is rational, which happens for any $N > k$. This only happens if $a_1 a_2 \cdots a_k = 1$.

Now let $f(x) = b_r X^r + b_{r-1} X^{r-1} + \cdots + b_0$ be a polynomial with integer coefficients which vanishes at $a_1, \ldots, a_k$. Clearly $b_r a_1, \ldots, b_r a_k$ are algebraic integers, but then

$$b_r \left(\sqrt[n]{a_1} + \sqrt[n]{a_2} + \cdots + \sqrt[n]{a_k} \right) = \sqrt[n]{b_r^{n-1}} \left(\sqrt[n]{b_r a_1} + \sqrt[n]{b_r a_2} + \cdots + \sqrt[n]{b_r a_k} \right)$$

is also an algebraic integer. Because it is also a rational number, we deduce that it is a rational integer. Consequently,

$$(Y_n)_{n \geq 1} = \left(b_r \left(\sqrt[n]{a_1} + \sqrt[n]{a_2} + \cdots + \sqrt[n]{a_k} \right) \right)_{n \geq 1}$$

is a sequence of positive integers. Because it converges to kb_r, it eventually becomes equal to kb_r (from a rank). Thus, there is a n such that

$$\sqrt[n]{a_1} + \sqrt[n]{a_2} + \cdots + \sqrt[n]{a_k} = k.$$

As $a_1 a_2 \cdots a_k = 1$, the AM-GM inequality implies that $a_1 = a_2 = \cdots = a_k = 1$.

Chapter 8
Cyclotomic Polynomials

Cyclotomic polynomials play a fundamental role in various areas of mathematics, bridging classical and modern theory. Their study dates back to Gauss, whose work laid the foundation for understanding these polynomials' deep connections to algebra and number theory. In algebra, for instance, cyclotomic polynomials appear in Witt's proof of Wedderburn's little theorem asserting that every finite division ring is a field. More recently, in number theory, they provide a foundation for the "cyclotomic criterion" used in the study of primitive divisors of Lucas and Lehmer sequences [71].

In addition to their purely theoretical significance, cyclotomic polynomials have also found applications in public-key cryptographic protocols. For instance, Lenstra showed that cyclotomic polynomials can be used to construct efficient discrete logarithm cryptosystems over finite fields [182]. Lately these polynomials have become foundational in lattice-based cryptography, where cyclotomic fields and polynomials play a central role in constructing lattices in which hard problems are believed to be resistant to quantum attacks. Specifically, Lyubashevsky, Peikert, and Regev's [184] and Langlois and Stehlé [169] work on ideal lattices and learning with errors over rings demonstrated the use of cyclotomic fields in developing cryptographic systems that leverage the hardness of certain lattice problems.

For a start, we mention that cyclotomic polynomials play a key role in the proof of the following classical results in number theory:

1) (Gauss-Wanzel) It is possible to construct the regular n-gon with a straightedge and compass if and only if n has the form $2^k p_1 p_2 \cdots p_r$, where $k \geq 0$ and the p_j's are distinct Fermat primes.
2) (Dirichlet) Let n be a positive integer. Then there exist infinitely many prime numbers p with $p \equiv 1 \pmod{n}$.

The chapter also explores the n-th inverse cyclotomic polynomial, which is defined as the quotient of $x^n - 1$ by the n-th cyclotomic polynomial. The investigation of these polynomials originates in the work of Moree [204] with particular focus on their coefficients.

Some key references devoted to cyclotomic polynomials and their coefficients are [59], [60], [107], [185], [186], [187] or [255]. Other important results concerning the coefficients of cyclotomic polynomials and their properties have also featured in the works [62], [63], [64], [87], [103] and [166]. This chapter is based mostly on the results in [20], [23], [24], [29], [30], [207] and the references therein.

Before providing specific details about cyclotomic polynomials, we first present some important examples of arithmetic functions used in this chapter. This digression will conclude with a description of the Möbius μ function and the associated inversion formula.

8.1 Arithmetic functions

In this section present some important arithmetic functions, inspired by the excellent book of [120]. Most of the times, by arithmetic functions people mean functions defined on $\mathbb{N}$, but it is not uncommon to refer to functions defined on $\mathbb{Z}$ or on $\mathbb{Q}$ as arithmetic. The constant and the identity functions defined on $\mathbb{N}$ are trivial examples of arithmetic functions.

Some classical examples of arithmetic functions appearing frequently in number theory are as follows.

Example 8.1. *The number of divisors function* $\tau : \mathbb{N}^\times \to \mathbb{N}^*$, *where*

$$\tau(n) = \#\{d \in \mathbb{N}^* : d \text{ is a divisor of } n\}.$$

Example 8.2. *The last digit function* $u : \mathbb{N}^* \to \mathbb{N}$, *with* $u(n) =$ *the last digit of* n.

Two important classes of arithmetic functions behave naturally with respect to the two fundamental operations on whole numbers.

An arithmetic function is called **additive** if $f(mn) = f(m) + f(n)$, for all m, n such that $\gcd(m,n) = 1$.

Example 8.3. *Let* p *be a prime. Then for every* $n \in \mathbb{N}^*$ *we denote by* $v_p(n)$ *the natural number such that* $p^{v_p(n)} \mid n$, *but* $p^{v_p(n)+1} \nmid n$. *It is clear to see that for any positive integers* m, n *we have* $v_p(mn) = v_p(m) + v_p(n)$, *hence* v_p *is an additive function. In the literature,* v_p *appears under the name p-adic valuation.*

Another important subcategory of arithmetic functions are the so-called **multiplicative functions**. An arithmetic function f is called multiplicative if

$$f(mn) = f(m)f(n) \text{ for all } m, n \in \mathbb{N} \text{ such that } \gcd(m,n) = 1. \tag{8.1}$$

If f satisfies (8.1) for any integers $m, n > 0$, then it is **totally multiplicative**.

Example 8.4. *If $n = p_1^{e_1} \cdots p_k^{e_k}$ is a positive integer written in its prime-power factorization, then it is not hard to count that the number of divisors $\tau(n) = (e_1 + 1) \cdot \cdots \cdot (e_k + 1)$. Using this representation, one can see immediately that τ is multiplicative. However, $\tau(9) = 3$, whereas $\tau(3) \cdot \tau(3) = 4$. This shows that τ is not totally multiplicative.*

The constant and the identity functions are totally multiplicative.

Example 8.5. *The function $f : \mathbb{N}^* \to \mathbb{N}^*$, where $f(n) = 2n$ is not multiplicative.*

Multiplicative functions play a key role in number theory, since in order to compute the values of the function at any positive integer n, it is enough to know the values of the function on the prime powers that divide n. To be precise, let $n = p_1^{e_1} \cdots p_k^{e_k}$ be the factorization prime-power factorization of n. If f is a multiplicative function, then using (8.1) inductively, we get

$$f(n) = f(p_1^{e_1}) \cdots f(p_k^{e_k}).$$

Suppose f is a multiplicative function and suppose that $f(n) \neq 0$ for some positive integer n. Then, using (8.1) we get that $f(n) = f(n)f(1)$, hence $f(1) = 1$. This shows that for any multiplicative function f, either $f(1) = 1$ or $f(n) = 0$ for all positive integers n.

Moreover, it is worth noting that the set of multiplicative functions forms a monoid with respect to the (pointwise) multiplication of functions. This is because the constant function 1 is (totally) multiplicative and, it is easy to show that if f and g are multiplicative functions, then so is their pointwise product, i.e. the function $n \mapsto f(n)g(n)$ for all n.

For any positive integer n, let us denote by $\varphi(n)$ the cardinality of the set

$$\{m \in \mathbb{N} : 1 \leq m \leq n \text{ and } \gcd(m,n) = 1\}.$$

Denoted φ, this satisfies $\varphi(1) = 1$ and is in fact a famous arithmetic function, called **Euler's Totient Function**, which plays a central role in number theory.

Suppose m, n are coprime positive integers. Then, by the Chinese Remainder Theorem, there is an isomorphism of rings

$$\mathbb{Z}/mn\mathbb{Z} \cong (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/mn\mathbb{Z}),$$

which gives rise to an isomorphism between their unit groups

$$(\mathbb{Z}/mn\mathbb{Z})^\times \cong (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times.$$

As the units in every ring $\mathbb{Z}/n\mathbb{Z}$ correspond bijectively with the positive integers less than or equal to n which are coprime to n, the group isomorphism above implies $\varphi(mn) = \varphi(m)\varphi(n)$ for every coprime positive integers m, n. This shows that the Euler Totient function φ is multiplicative. However, it is easy to check that φ is not totally multiplicative.

This fact, together with a remark above, implies that in order to evaluate $\varphi(n)$ it is enough to evaluate $\varphi(p^e)$ for all distinct prime-powers p^e appearing in the factorization of n. Now, if p is prime, then $\gcd(m,p^e)=1$ if and only if $\gcd(m,p)=1$. In that case, we see that

$$\begin{aligned}\varphi(p^e) &= \#\{m : 1 \le m \le p^e\} - \#\{m : 1 \le m \le p^e \text{ and } p \mid m\} \\ &= p^e - p^{e-1},\end{aligned}$$

where for a set A we denoted by $\#A$ its cardinal.

We therefore have the following representations for $\varphi(n)$

$$\varphi(n) = \prod_{i=1}^{k}\left(p_i^{e_i} - p_i^{e_i-1}\right) = \prod_{i=1}^{k} p^{e_i}\left(1-\frac{1}{p_i}\right) = n\prod_{i=1}^{k}\left(1-\frac{1}{p_i}\right), \tag{8.2}$$

where $n = p_1^{e_1}\cdots p_k^{e_k}$ is the factorization prime-power factorization of n.

We remark that this property was proved in section 4.9, using the inclusion-exclusion principle. To emphasize the utility of this representation, we prove the following inequality involving Euler's totient function.

Example 8.6. *For every composite number $n \in \mathbb{N}^*$, show that*

$$\varphi(n) \le n - \sqrt{n}.$$

Solution. Denote by $p_1, p_2, \ldots, p_k$ the set of all prime distinct divisors of n. Since n is composite, there exists a $j \in \{1,2,\ldots,k\}$ such that $p_j \le \sqrt{n}$.

Applying the previous formula, we deduce that

$$\varphi(n) = n\left(1-\frac{1}{p_1}\right)\cdots\left(1-\frac{1}{p_k}\right) \le n\left(1-\frac{1}{p_j}\right) \le n\left(1-\frac{1}{\sqrt{n}}\right) = n-\sqrt{n},$$

which is what we had to show.

Theorem 8.1. *For any given multiplicative function f, the function*

$$F(n) = \sum_{d\mid n} f(d)$$

is multiplicative.

Before showing the proof of the theorem, let us give a few applications.

Corollary 8.1. *The number of divisor function can be written as $\tau(n) = \sum_{d\mid n} 1$, for all $n \in \mathbb{N}^*$. As the constant function 1 is clearly (totally) multiplicative, it follows from the theorem above that τ is multiplicative.*

In the following corollary it is perhaps more difficult to give a direct proof of the multiplicative property of the function.

Corollary 8.2. *Let $\sigma : \mathbb{N}^* \to \mathbb{N}^*$ be the sum of divisors function. Ideed, for any n we have that $\sigma(n) = \sum_{d|n} d$. As the identity function is multiplicative, the previous theorem implies that σ is also multiplicative.*

The next problem involves the sum of divisors function.

Example 8.7 (St. Petersburg Olympiad). *Find all the solutions $n, m, k \in \mathbb{N}^*$ of*

$$\sigma(n)^k = n^m.$$

Solution. Note that if $n = 1$, then every $m, k \in \mathbb{N}^*$ satisfy the equality.

Suppose that the triple $(n, m, k) \in \mathbb{N}^*$ is a solution such that $n > 1$, while $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_t^{\alpha_t}$ is the factorisation of n into distinct prime powers. As $\sigma(n) \geq n + 1$, we deduce that $k < m$. Therefore, $\sigma(n) = n^{\frac{m}{k}}$. It follows that $\sigma(n) = p_1^{\beta_1} p_2^{\beta_2} \cdots p_t^{\beta_t}$, where $\beta_i \geq \alpha_i + 1$, for all $i \in \{1, 2, \ldots, t\}$. First, note that

$$\sigma(n) \geq p_1^{\alpha_1+1} p_2^{\alpha_2+1} \cdots p_t^{\alpha_t+1}.$$

Secondly, note that for every $i \in \{1, 2, \ldots, t\}$, we have that $p_i^{\alpha_i+2} + 1 > 2p_1^{\alpha_i+1}$, which implies that $p_i^{\alpha_i+2} - p_i^{\alpha_i+1} > p_i^{\alpha_i+1} - 1$. From here we deduce that for all such i,

$$p_i^{\alpha_i+1} > \frac{p_i^{\alpha_i+1} - 1}{p_i - 1} = \sigma(p_i^{\alpha_i}).$$

One can therefore derive the chain of inequalities

$$\sigma(n) \geq p_1^{\alpha_1+1} p_2^{\alpha_2+1} \cdots p_t^{\alpha_t+1} > \sigma(p_1^{\alpha_1}) \sigma(p_2^{\alpha_2}) \cdots \sigma(p_t^{\alpha_t}) = \sigma(n),$$

a contradiction. To justify the last equality, we use the fact that σ is a multiplicative function. Hence, the given Diophantine equation has solutions only when $n = 1$, when any $m, k \in \mathbb{N}^*$ satisfy the equation.

We now present an inequality that involves both functions τ and σ, the number and sum of divisors functions.

Example 8.8. *For every integer $n \geq 2$, show that the following inequality holds*

$$\frac{\sigma(n)}{\tau(n)} \geq \sqrt{n}.$$

Solution. Let $d_1, d_2, \ldots, d_{\tau(n)}$ be the positive divisors of n. These can be written (by changing their order) as $\frac{n}{d_1}, \frac{n}{d_2}, \ldots, \frac{n}{d_{\tau(n)}}$.

Therefore, the square of the sums of divisors of n can be written as

$$\sigma^2(n) = \left(\frac{n}{d_1} + \frac{n}{d_2} + \cdots + \frac{n}{d_{\tau(n)}}\right)\left(d_1 + d_2 + \cdots + d_{\tau(n)}\right),$$

hence

$$\sigma^2(n) = n\left(\frac{1}{d_1} + \frac{1}{d_2} + \cdots + \frac{1}{d_{\tau(n)}}\right)\left(d_1 + d_2 + \cdots + d_{\tau(n)}\right).$$

Applying the Cauchy-Buniakowski-Schwarz inequality for the last two terms in the product on the right, we get that $\sigma^2(n) \geq n\tau^2(n)$, which is equivalent to the inequality in the statement.

Example 8.9. *The Euler Totient function φ, the number of divisors τ and the sum od divisors σ, satisfy the following inequality*

$$\varphi(n) + \sigma(n) \leq n\tau(n),$$

for any positive integer $n \geq 2$. The equality holds if and only if n is a prime number.

Solution. First note that the inequality holds (trivially) with equality if $n = p$ is a prime number. Moreover, one can immediately check that the inequality holds strictly if $n = p^k$, $k \geq 2$ is a prime power. To prove the inequality for general n, we are going to use strong induction.

Note that the inequality is true for $n = 2$ and assume that the inequality holds for every n such that $2 \leq n \leq k$. We are going to prove that the inequality holds for k. If k is a prime power, we are done by the remark in the first paragraph. Otherwise, we can write $k = ab$, where $1 < a, b < k$ and $\gcd(a, b) = 1$. As the functions φ, σ and τ are multiplicative, we have

$$\varphi(k) + \sigma(k) = \varphi(ab) + \sigma(ab) = \varphi(a)\varphi(b) + \sigma(a)\sigma(b).$$

the right-hand side is strictly less than $(\varphi(a) + \sigma(a))(\varphi(b) + \sigma(b))$.

Now, using the inductive hypothesis we get that

$$(\varphi(a) + \sigma(a))(\varphi(b) + \sigma(b)) \leq a\tau(a)b\tau(b) = ab\tau(ab) = k\tau(k),$$

which completes the induction. Looking carefully at the inequalities derived above, one can easily justify the claimed equality case.

We have seen that the Euler totient function is multiplicative. Let us now prove an identity which, combined with the previous theorem, allows one to give an indirect proof of the fact that the identity function is multiplicative.

Example 8.10. *For every $n \in \mathbb{N}^*$, we have $n = \sum_{d|n} \varphi(d)$.*

Solution. By partitioning the set $\{1,2,\ldots,n\}$ into the disjoint sets given by $M_d = \{1 \leq i \leq n \mid \gcd(i,n) = d\}$ for every positive divisor d of n. Note that

$$n = \sum_{d|n} |M_d|.$$

Let us now determine the cardinality of the set M_d. If $x \in M_d$, then the integers $\frac{x}{d}$ and $\frac{n}{d}$ are coprime. In fact, this gives rise to a one-to-one correspondence between the sets M_d and $\{1 \leq i \leq n/d \mid \gcd(i,n/d) = 1\}$. This shows that $|M_d| = \varphi(n/d)$, hence

$$n = \sum_{d|n} \varphi\left(\frac{n}{d}\right) = \sum_{d|n} \varphi(d),$$

where the last equality follows by changing the order of summation.

We now return to the proof of Theorem 8.1.

Proof (of Theorem 8.1). Let m,n be positive integers with $\gcd(m,n) = 1$. Then, all divisors d of the product mn can be written as $d = ab$, where $a \mid m$ and $b \mid n$. Since $\gcd(a,b) \mid \gcd(m,n)$ two such integers a,b are also coprime. Using the fact that f is multiplicative, we see that for any such $d = ab$, we can write $f(d) = f(a)f(b)$ and therefore

$$F(mn) = \sum_{d|mn} f(d) = \sum_{a|m,b|n} f(ab) = \sum_{a|m} f(a) \sum_{m|b} f(b) = F(m)F(n).$$

The conclusion follows. □

This raises some natural questions. For every multiplicative function F, does there exists a multiplicative function f such that $F(n) = \sum_{d|n} f(d)$ for all n? And if yes, given F is the function f unique? The Möbius μ function, which we discuss in the next section allows us to answer these questions.

8.2 The Möbius μ function

The Möbius μ function can be defined multiplicatively on $\mathbb{N}^*$ by just specifying its values on prime powers. If p is a prime number, define $\mu(p) = -1$ and $\mu(p^k) = 0$ for every $k \geq 2$. Now the value $\mu(n)$ can be computed recursively for any $n \in \mathbb{N}^*$.

Since we defined μ as a multiplicative function, we have that $\mu(1) = 1$. Moreover, one can easily check that $\mu(2) = -1$, $\mu(3) = -1$, $\mu(4) = 0$, then $\mu(5) = -1$, $\mu(6) = \mu(10) = 1$ and $\mu(7 \cdot 11 \cdot 17) = -1$.

It is easy to deduce that for any $n \in \mathbb{N}^*$, we have

$$\sum_{d|n} \mu(d) = \begin{cases} 1, \text{ if } n = 1, \\ 0, \text{ otherwise.} \end{cases} \tag{8.3}$$

Indeed, the result follows trivially for $n = 1$. If $n = p^k$ is prime power then the sum consists of $\mu(1) + \mu(p) = 1 + (-1) + 0 + \cdots + 0$, where the sum on the right has $k + 1$ terms. In general, denote by

$$F(n) = \sum_{d|n} \mu(d).$$

By Theorem 8.1, it follows that F is a multiplicative function. Since we saw that F vanishes on prime-powers, it follows that $F(n) = 0$ for any $n \geq 2$.

We give another proof of the formula for the Euler totient function $\varphi(n)$.

Example 8.11. *Show that for any $n \in \mathbb{N}^*$, we have*

$$\varphi(n) = n \sum_{d|n} \frac{\mu(d)}{d}.$$

Solution. Since $\varphi(n)$ gives counts the numbers that are less than n and coprime to n. So we can write

$$\varphi(n) = \sum_{k=1}^{n} \begin{cases} 1, \text{ if } (k,n) = 1, \\ 0, \text{ otherwise.} \end{cases}$$

Formula (8.3) allows one to write

$$\sum_{d|k \text{ and } d|n} \mu(d) = \begin{cases} 1, \text{ if } (k,n) = 1, \\ 0, \text{ otherwise} \end{cases},$$

therefore by replacing into the formula above we have

$$\varphi(n) = \sum_{k=1}^{n} \sum_{d|k \text{ and } d|n} \mu(d).$$

By first changing the order of summation, we obtain

$$\varphi(n) = \sum_{d|n} \mu(d) \sum_{1 \leq k \leq n, d|k} 1 = \sum_{d|n} \mu(d) \frac{n}{d}.$$

In the formula $\varphi(n) = n \sum_{d|n} \frac{\mu(d)}{d}$ from the example above, if we denote by $r = n/d$, we can see the right hand side as a sum over all possible factorizations of $n = dr$, where d and r are positive integers.

In other words,

$$\varphi(n) = \sum_{d,r\geq 1, n=dr} \mu(d) r. \tag{8.4}$$

Recall that in Example 8.10 we saw

$$n = \sum_{d|n} \varphi(d) = \sum_{d,r\geq 1, n=dr} \varphi(d) \cdot 1. \tag{8.5}$$

Identities (8.4) and (8.5) are particular instances of a more general result.

Theorem 8.2 (Möbius inversion formula). *For any two arithmetic functions f and g we have*

$$g(n) = \sum_{ab=n} f(b) \text{ for every integer } n \geq 1$$

if and only if

$$f(m) = \sum_{cd=m} \mu(c) g(d) \text{ for every integer } m \geq 1.$$

The conclusion of the theorem is frequently written shortly as follows

$$g(n) = \sum_{d|n} f(d) \text{ for every } n \geq 1 \Leftrightarrow f(m) = \sum_{d|m} \mu(m/d) g(d) \text{ for every } m \geq 1.$$

Proof. If $g(n) = \sum_{ab=n} f(b)$, for all positive integers n, then

$$\sum_{cd=m} \mu(c) g(d) = \sum_{cd=m} \mu(c) \sum_{ab=d} f(b) = \sum_{abc=m} \mu(c) f(b)$$

which is further equal to

$$\sum_{b|m} f(b) \sum_{ac=m/b} \mu(c) = f(m),$$

as desired. In the last equality we used the fact that the sum on the right is zero unless $\frac{m}{b} = 1$, which was explained in (8.3).

Conversely, if

$$f(m) = \sum_{cd=m} \mu(c) g(d),$$

for all positive integers m, then

$$\sum_{ab=n} f(b) = \sum_{ab=n} \sum_{cd=b} \mu(c) g(d) = \sum_{acd=n} \mu(c) g(d) = \sum_{d|n} g(d) \cdot \sum_{ac=n/d} \mu(c).$$

As in the first part, the relation (8.3) allows us to deduce that the second sum in the last expression vanishes unless $\frac{n}{d} = 1$. The conclusion follows immediately. □

The examples above, together with this theorem serve as motivation for defining the following concept. Given two multiplicative functions f, g, we define their convolution $f * g$ as follows

$$(f * g)(n) = \sum_{ab=n} f(a)f(b) \text{ for every } n \in \mathbb{N}^*.$$

The set of arithmetic multiplicative functions, together with the convolution operation forms a commutative monoid, where the identity element is the δ function, defined as

$$\delta(n) = \begin{cases} 1, \text{ if } n = 1, \\ 0, \text{ otherwise.} \end{cases}$$

We will restrict ourselves to proving the fact that the set of multiplicative functions is closed with respect to the convolution operation, leaving the proofs of the other axioms of a monoid to the curious reader.

Indeed, suppose f and g are two multiplicative functions. Let m, n be two coprime integers. Note that by definition

$$(f * g)(mn) = \sum_{ab=mn} f(a)g(b).$$

It is easy to show that there exists integers r, s, t, u, such that $\gcd(r, s) = 1$ and $\gcd(t, u) = 1$ such that $a = rs$,$b = tu$, $m = rt$ and $n = su$. Using this, note that $f(a) = f(rs) = f(r)f(s)$ and $g(b) = g(tu) = g(t)g(u)$.

We then have

$$(f * g)(mn) = \sum_{rt=m, su=n} f(rs)g(tu) = \sum_{rt=m} f(r)g(t) \sum_{su=n} f(s)g(u)$$

and the right-hand side is easily seen to be equal to $(f * g)(m) \cdot (f * g)(n)$. Since m, n are two arbitrarily chosen coprime numbers, this shows that $f * g$ is a multiplicative function.

This observation about the convolution of two multiplicative functions, together with Theorems 8.1 and 8.2, allows us to give a positive answer to the two questions raised at the end of the previous section.

Indeed, if F is a multiplicative arithmetic function, then the function $f(m) = \sum_{d|m} \mu(m/d)F(d)$ is multiplicative. This is because f can be seen as the convolution between the multiplicative functions μ and F. Now, Theorem 8.2 guarantees that $F(n) = \sum_{d|n} f(d)$. The uniqueness of f follows immediately from the direct implication of the aforementioned theorem.

8.3 Ramanujan sums

For every positive integers n and q, the Ramanujan sum $\rho(n,q)$ is defined as

$$\rho(n,q) = \sum_{\gcd(a,n)=1} e^{2\pi i \frac{a}{n} q}, \tag{8.6}$$

where the sum is taken over all a such that $1 \leq a \leq n$ and $\gcd(a,n) = 1$.

While a usual notation for the Ramanujan sums is $c_n(q)$, we avoid this as a similar notation is used for the coefficients of cyclotomic polynomials. Another motivation for our choice is that by fixing one of q or n, one can think of Ramanujan sums as arithmetic functions of the remaining free variable.

We start by remarking that, by fixing $n \in \mathbb{N}^*$, the arithmetic function $\rho(n,\cdot) : \mathbb{N}^* \to \mathbb{C}$ is periodic, as $\rho(n,q+n) = \rho(n,q)$, for all $q \in \mathbb{N}$.

In what follows, we see that fixing q and regarding $\rho(\cdot,q) : \mathbb{N}^* \to \mathbb{C}$ as a function in the variable n will unravel some remarkable properties. For example, notice that when $q = 0$, one obtains the Euler Totient function, i.e. $\rho(n,0) = \varphi(n)$ for all $n \in \mathbb{N}^*$.

Let us also present the following identity which is useful in the later computations involving Ramanujan sums.

Example 8.12. *For $q \in \mathbb{Z}$, and every positive integer n, we consider the function $\delta_q(n) = \sum_{a=1}^{n} e^{\frac{2\pi a}{n} \cdot i \cdot q}$. We have the following identity*

$$\delta_q(n) = \begin{cases} n \text{ if } n \mid q \\ 0 \text{ if } n \nmid q \end{cases}.$$

Solution. Indeed, if $n \mid q$ then all terms in the sum are 1 and the conclusion follows. Otherwise, let $n = d \cdot n'$, $q = d \cdot q'$, where $d = \gcd(n,q)$. We have

$$\sum_{a=1}^{n} e^{2\pi i \frac{aq}{n}} = \sum_{a=1}^{n} e^{2\pi i \frac{aq'}{n'}}.$$

As q' and n' are coprime, exponentiation by q' is an automorphism of the group of n'-th roots of unity. Therefore, the last sum is

$$\sum_{a=1}^{n} e^{2\pi i \frac{a}{n'}} = d \sum_{a=1}^{n'} e^{2\pi i \frac{a}{n'}}.$$

By Viéta's formula applied to the polynomial $X^{n'} - 1$, the sum vanishes.

Suppose $q \in \mathbb{N}^*$ is fixed. An immediate corollary of the example above is that $\delta_q : \mathbb{N}^* \to \mathbb{N}$ is a multiplicative function. Indeed, suppose $m, n \in \mathbb{N}^*$ are coprime. Then, as $nm \mid q$ if and only if $n \mid q$ and $m \mid q$ it follows that

$$\delta_q(nm) = \delta_q(n)\delta_q(m). \tag{8.7}$$

Theorem 8.3 (Kluyver). *Let $q \in \mathbb{N}^*$ be fixed. Then*

$$\rho(n,q) = \sum_{d|\gcd(n,q)} d\mu\left(\frac{n}{d}\right) \text{ for all } n \in \mathbb{N}^*. \tag{8.8}$$

Proof. In the previous example we saw that for all $n \in \mathbb{N}^*$, we have

$$\delta_q(n) = \sum_{a=1}^{n} e^{2\pi i \frac{aq}{n}} = \begin{cases} n \text{ if } n \mid q \\ 0 \text{ if } n \nmid q \end{cases}.$$

This can be written as

$$\delta_q(n) = \sum_{d|n} \sum_{(a,d)=1} e^{2\pi i \frac{q\cdot a\cdot n}{d}} = \sum_{d|n} \sum_{(a,d)=1} e^{2\pi i \frac{aq}{d}} = \sum_{d|n} \rho(d,q).$$

Applying Möbius inversion formula, we obtain (Theorem 8.2)

$$\rho(n,q) = \sum_{d|n} \delta_q(d)\mu\left(\frac{n}{d}\right) = \sum_{d|\gcd(n,q)} d\mu\left(\frac{n}{d}\right). \qquad \square \tag{8.9}$$

With the convention that $\mu\left(\frac{n}{d}\right) = 0$ if $d \nmid n$, we obtain the following immediate consequences of formula (8.8), valid for all $n \in \mathbb{N}^*$:

$$\begin{aligned}
\rho(n,1) &= \mu(n);\\
\rho(n,2) &= \sum_{d|\gcd(n,2)} d\mu\left(\frac{n}{d}\right) = \mu(n) + 2\mu(n/2);\\
\rho(n,3) &= \sum_{d|\gcd(n,3)} d\mu\left(\frac{n}{d}\right) = \mu(n) + 3\mu(n/3);\\
\rho(n,4) &= \sum_{d|\gcd(n,4)} d\mu\left(\frac{n}{d}\right) = \mu(n) + 2\mu(n/2) + 4\mu(n/4);\\
\rho(n,5) &= \sum_{d|\gcd(n,5)} d\mu\left(\frac{n}{d}\right) = \mu(n) + 5\mu(n/5);\\
\rho(n,6) &= \sum_{d|\gcd(n,6)} d\mu\left(\frac{n}{d}\right) = \mu(n) + 2\mu(n/2) + 3\mu(n/3) + 6\mu(n/6);\\
\rho(n,7) &= \sum_{d|\gcd(n,7)} d\mu\left(\frac{n}{d}\right) = \mu(n) + 7\mu(n/7);\\
\rho(n,8) &= \sum_{d|\gcd(n,8)} d\mu\left(\frac{n}{d}\right) = \mu(n) + 2\mu(n/2) + 4\mu(n/4) + 8\mu(n/8).
\end{aligned}$$

In addition, one can now derive the following corollary.

Corollary 8.3. *For $q \in \mathbb{N}^*$ fixed, the function $\rho(\cdot, q) : \mathbb{N}^* \to \mathbb{C}$ is multiplicative.*

Proof. Indeed, we derived in 8.9, that for any $n \in \mathbb{N}^*$,

$$\rho(n,q) = \sum_{d|n} \delta_q(d)\mu\left(\frac{n}{d}\right).$$

As the right-hand-side is the convolution product $\delta_q * \mu$ of two multiplicative functions, it follows from the results in the previous section that $\rho(\cdot, q)$ is also a multiplicative function. □

We saw that the values of a multiplicative function are fully determined by the values these functions take on prime powers. Let us describe these.

Suppose $q \in \mathbb{N}^*$ is fixed. Then, for every prime number p and for every positive integer k, Theorem 8.3 yields

$$\rho(p^k, q) = \sum_{d|\gcd(p^k,q)} d\mu\left(\frac{p^k}{d}\right) = \begin{cases} p^k - p^{k-1}, \text{ if } p^k \mid q \\ -p^{k-1}, \text{ if } p^{k-1} \mid q \text{ but } p^k \nmid q \\ 0, \text{ otherwise.} \end{cases}$$

In particular, $\rho(\cdot, q)$ takes integral values on powers of primes. Then, by Corollary 8.3, $\rho(\cdot, q)$ are integral valued arithmetic functions, for all $q \in \mathbb{N}^*$.

Example 8.13. *Another interesting situation is when $n = p_1 p_2 \cdots p_k$ is a product of distinct k primes. Without loosing generality, suppose that $\gcd(n,q) = p_1 p_2 \cdots p_m$, where $m \leq k$. The theorem presented above together with the definition of the Möbius function yield that*

$$\rho(n,q) = \sum_{i=1}^{m} (-1)^{k-i} S_i(p_1, p_2, \ldots, p_m),$$

where S_i is the i-th fundamental symmetric polynomial in m variables.

Theorem 8.4 (Von Sterneck). *The following formula holds*

$$\rho(n,j) = \frac{\mu\left(\frac{n}{\gcd(n,j)}\right)\varphi(n)}{\varphi\left(\frac{n}{\gcd(n,j)}\right)}. \tag{8.10}$$

Proof. The fact that for fixed j, $\rho(\cdot, j) : \mathbb{N} \to \mathbb{R}$ is multiplicative can be seen for instance on page 16 of [233]. In addition, we remark that for fixed j, the functions $n \mapsto \mu\left(\frac{n}{\gcd(n,j)}\right)$, $n \mapsto \varphi\left(\frac{n}{\gcd(n,j)}\right)$ are multiplicative and so is the Euler totient function φ. Hence, it follows that the formula (8.10) holds for every positive integers n and j. □

The right-hand side of (8.10) often appears under the name of Von Sterneck's function and the first proof of the equality in (8.10) is due to Hölder (see the discussion on page 243 of [127]).

Let us now see two example problems involving Ramanujan sums.

Example 8.14. *For every $n \in \mathbb{N}^*$, prove that the following identities hold*

$$\sum_{\gcd(k,n)=1} \cos\frac{2k\pi}{n} = \mu(n) \text{ and } \sum_{\gcd(k,n)=1} \sin\frac{2k\pi}{n} = 0,$$

where the summation is over all integers $1 \leq k \leq n$ which are coprime to n.

Solution. We have

$$\sum_{\gcd(k,n)=1} \cos\frac{2k\pi}{n} + i \sum_{\gcd(k,n)=1} \sin\frac{2k\pi}{n} = \sum_{\gcd(k,n)=1} e^{2\pi i \frac{k}{n}} = \rho(n,1) = \mu(n),$$

so the identities follow by identifying the real and the imaginary parts.

We now present another interesting identity using Ramanujan sums.

Example 8.15. *For every $n \in \mathbb{N}^*$, prove that the following identity holds*

$$\sum_{\gcd(k,n)=1} \cos^2\frac{2k\pi}{n} = \frac{1}{2}\varphi(n) + \frac{1}{2}\mu(n) + \mu\left(\frac{n}{2}\right).$$

Solution. For every such n, we have that

$$\rho(n,2) = \sum_{\gcd(k,n)=1} e^{4\pi i \frac{k}{n}} = \sum_{\gcd(k,n)=1} \left(\cos\frac{4k\pi}{n} + i\sin\frac{4k\pi}{n}\right),$$

hence, using the fact that $\rho(n,2)$ is real-valued (actually integer-valued),

$$\sum_{\gcd(k,n)=1} \cos\frac{4k\pi}{n} = \rho(n,2) \text{ and } \sum_{\gcd(k,n)=1} \sin\frac{4k\pi}{n} = 0.$$

Therefore, using the double-angle formula for the cosine function,

$$\sum_{\gcd(k,n)=1} \cos^2\frac{2k\pi}{n} = \sum_{\gcd(k,n)=1} \frac{1+\cos\frac{4k\pi}{n}}{2} = \frac{1}{2}\left(\varphi(n) + \rho(n,2)\right).$$

The conclusion follows from (8.8), using that $\mu(n/2) = 0$ if n is odd.

Remark. Clearly, it follows that

$$\sum_{\gcd(k,n)=1} \sin^2\frac{2k\pi}{n} = \sum_{\gcd(k,n)=1} \left(1 - \cos^2\frac{2k\pi}{n}\right) = \frac{1}{2}\varphi(n) - \frac{1}{2}\mu(n) - \mu\left(n/2\right).$$

8.4 Cyclotomic polynomials: definition and basic properties

For an integer $n \geq 1$, recall that an nth root ζ is called primitive if $\zeta^n = 1$, but $\zeta^d \neq 1$ for all $1 \leq d < n$. The n-th cyclotomic polynomial Φ_n is defined by

$$\Phi_n(z) = \prod_{\zeta^n=1} (z - \zeta) = \sum_{j=0}^{\varphi(n)} c_j^{(n)} z^j, \tag{8.11}$$

where ζ are the n-th order primitive roots of unity, and φ is Euler's totient function, which is also the degree of the polynomial. The term **cyclotomic** comes from the property of the nth roots of unity to divide the unit circle into n equal arcs, forming a regular polygon inscribed in the unit circle.

The first few cyclotomic polynomials are

$$\begin{aligned}
&\Phi_1(z) = z - 1,\ \Phi_2(z) = z + 1,\ \Phi_3(z) = z^2 + z + 1,\ \Phi_4(z) = z^2 + 1,\\
&\Phi_5(z) = z^4 + z^3 + z^2 + z + 1,\ \Phi_6(z) = z^2 - z + 1,\\
&\Phi_7(z) = z^6 + z^5 + z^4 + z^3 + z^2 + z + 1,\ \Phi_8(z) = z^4 + 1,\\
&\Phi_9(z) = z^6 + z^3 + 1,:\ \Phi_{10}(z) = z^4 - z^3 + z^2 - z + 1,\\
&\Phi_{12}(z) = z^4 - z^2 + 1,\ \Phi_{14}(z) = z^6 - z^5 + z^4 - z^3 + z^2 - z + 1,\\
&\Phi_{15}(z) = z^8 - z^7 + z^5 - z^4 + z^3 - z + 1,\ \Phi_{16}(z) = z^8 + 1,\\
&\Phi_{18}(z) = z^6 - z^3 + 1,\ \Phi_{20}(z) = z^8 - z^6 + z^4 - z^2 + 1,\\
&\Phi_{21}(z) = z^{12} - z^{11} + z^9 - z^8 + z^6 - z^4 + z^3 - z^1 + 1.
\end{aligned} \tag{8.12}$$

Using the Möbius function μ, an alternative version of (8.11) is obtained by the multiplicative version of the Möbius inversion formula, as

$$\Phi_n(z) = \prod_{d|n} \left(z^d - 1\right)^{\mu(n/d)}. \tag{8.13}$$

The following identity for products of cyclotomic polynomials is useful.

Theorem 8.5. *For every $n \in \mathbb{N}^*$, the following equality holds*

$$z^n - 1 = \prod_{d|n} \Phi_d(z), \tag{8.14}$$

where Φ_d is the d-th cyclotomic polynomial.

Proof. The roots of $z^n - 1$ are all n-th roots of unity. However, ζ is an n-th root of unity if and only if ζ is a primitive root of unity for exactly one positive divisor d of n. The roots of polynomials Φ_d are, by definition, exactly the primitive d-th roots of unity, so (8.14) holds because the polynomials on both sides are monic, having simple roots in one-to-one correspondence. □

As an application, we now present a shorter (but more conceptual) proof for the formula in Example 8.10.

Example 8.16. *For every $n \in \mathbb{N}^*$, we have*

$$n = \sum_{d|n} \varphi(d).$$

Solution Each polynomial Φ_d has degree $\varphi(d)$, so the identity follows by identifying the degrees on both sides in the formula (8.14).

It is well-known that every cyclotomic polynomial has integer coefficients and is irreducible over $\mathbb{Z}$ ([146, Theorem 1, p.195]).

Lemma 8.1. *The following properties are known:*
1° $\Phi_{pn}(z) = \Phi_n(z^p)$ *if p is a prime divisor of n.*
2° $\Phi_n(z) = z^{\varphi(n)}\Phi_n\left(\frac{1}{z}\right)$ *for $n > 1$.*
3° *For n odd one has $\Phi_{2n}(z) = \Phi_n(-z)$.*

Theorem 8.6. *Let p be a prime number and m be a positive integer. If p does not divide m, then $\Phi_{pm}(z)\Phi_m(z) = \Phi_m(z^p)$.*

Proof. Let d be an integer such that $d \mid pm$ and p does not divide d. Since p is prime, $\gcd(p,d) = 1$, hence $d \mid m$. Since p does not divide m, we have $\gcd(p,m) = 1$. If d is a divisor of m, then $\gcd(m/d, p) = 1$. Since function μ is multiplicative, it follows that

$$\mu(mp/d) = \mu(m/d)\,\mu(p) = -\mu(m/d).$$

Assume that $p \mid d$, in which case $d = pn$ for some integer n, where $n \mid m$, therefore $d \mid pm$. In these notations we obtain

$$\begin{aligned}
\Phi_{pm}(z)\Phi_m(z) &= \prod_{d|pm} \left(z^d - 1\right)^{\mu(pm/d)} \Phi_m(z) \\
&= \prod_{d|pm,\, p|d} \left(z^d - 1\right)^{\mu(pm/d)} \prod_{d|pm,\, p\nmid d} \left(z^d - 1\right)^{\mu(pm/d)} \Phi_m(z) \\
&= \prod_{n|m} (z^{pn} - 1)^{\mu(pm/pn)} \prod_{d|m} \left(z^d - 1\right)^{\mu(pm/d)} \Phi_m(z) \\
&= \Phi_m(z^p) \prod_{d|m} \left(z^d - 1\right)^{-\mu(m/d)} \Phi_m(z) \\
&= \Phi_m(z^p) \left(\Phi_m(z)\right)^{-1} \Phi_m(z) = \Phi_m(z^p).
\end{aligned}$$

□

By formula (8.11) the following interesting relations hold

$$\frac{\mathrm{d}\Phi_n(z)}{\mathrm{d}z} = \sum_{j=0}^{\varphi(n)-1} (\varphi(n)-j)\, c_j^{(n)} z^{\varphi(n)-j-1},$$

$$\frac{\mathrm{d}^\alpha \Phi_n(z)}{\mathrm{d}z^\alpha} = \sum_{j=0}^{\varphi(n)} \frac{(\varphi(n)-j)!\, c_j^{(n)}}{\Gamma(\varphi(n)-j-\alpha+1)} z^{\varphi(n)-j-\alpha}.$$

Definition 8.1. The **companion matrix** representation of a monic polynomial $P(z) = a_0 + a_1 z + \cdots + a_{m-1} z^{m-1} + z^m$, $m \geq 2$ is the square matrix

$$C(P(z)) = \begin{bmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & \cdots & 0 & -a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -a_{m-1} \end{bmatrix}.$$

The following tools can be defined for a general polynomial [76].

Definition 8.2. Let $m \geq 2$ and $P(z) = a_0 + a_1 z + \cdots + a_{m-1} z^{m-1} + a_m z^m$ be a polynomial with $a_0, \ldots, a_m \in \mathbb{R}$, having the factorization

$$P(z) = a_m (z-\alpha_1) \cdots (z-\alpha_m).$$

1° The **length** of the polynomial P is

$$L(P) = |a_0| + |a_1| + \cdots + |a_m| = \sum_{j=0}^{m} |a_j|.$$

2° The **height** of the polynomial P is

$$H(P) = \max_{j=0,1,\ldots,m} |a_j|.$$

3° The **Mahler measure** of the polynomial P is

$$M(P) = |a_m| \cdot \prod_{j=1}^{m} \max\{1, |\alpha_j|\}\, |a_j|.$$

The following results are known to connect these notions.

$$\frac{1}{\binom{m}{\lfloor m/2 \rfloor}} H(P) \leq M(P) \leq H(P)\sqrt{m+1},$$

$$L(P) \leq 2^m M(P) \leq 2^m L(P),$$

$$M(P) \leq L(P) \leq (m+1) H(P),$$

where $\binom{m}{\lfloor m/2 \rfloor}$ is the binomial coefficient.

Sometimes one may use $P_+ = \max_{j=0,1,\ldots,m} |a_j|$ and $P_- = \min_{j=0,1,\ldots,m} |a_j|$.

The following results presents some properties of the companion matrix for polynomials in general, and for cyclotomic polynomials in particular.

Proposition 8.1. *If $P(z) = a_0 + a_1 z + \cdots + a_{m-1} z^{m-1} + z^m$, then we have:*

1° *The characteristic polynomial of $C(P(z))$ is $P(z)$, hence the eigenvalues of the matrix $C(P(z))$ are the roots of $P(z)$.*

2° $\det(C(P(z))) = (-1)^m a_0$, *hence* $\det(C(\Phi_n(z))) = (-1)^{\varphi(n)} = 1$, $n \geq 3$.

3° $\mathrm{Tr}(P(z)) = -a_{m-1}$, *hence* $\mathrm{Tr}(\Phi_n(z)) = \mu(n)$.

The proof of item 3° follows from Theorem 8.9 or Theorem 8.16.

8.5 The coefficients of cyclotomic polynomials. Suzuki's Theorem

Many studies have been devoted to the coefficients of cyclotomic polynomials. As seen in (8.12), the first cyclotomic polynomials only have 0, 1 and -1 as coefficients. In fact, just in 1883 Mignotti found that -2 first appears in Φ_{105} as the coefficient of z^7, and moreover Φ_n only has the coefficients 0 and ± 1, whenever n is a product of at most two distinct primes. Next, the coefficient 2 first appears for $n = 165$, while all coefficients of P_n do not exceed 2 in absolute value for $n < 385$. Later, in 1895 Bang showed that for $n = pqr$ with $p < q < r$ odd primes, no coefficient of Φ_n is larger than $p - 1$. An important breakthrough came in 1931, when Schur showed that the coefficients of cyclotomic polynomials can be arbitrarily large in absolute value.

A history of early results can be found in [179]. Later, Suzuki [246] proved that any integer number can be a coefficient of a cyclotomic polynomial of a certain degree. For more details regarding the study of cyclotomic polynomials and their coefficients we refer the reader to papers by Erdös [110], [111], Ji [150], and to the monograph of Bachman[43]. The explicit computation of the coefficients of cyclotomic polynomials involves elaborated calculations [229, p.258-259].

In what follows, we present the aforementioned result of Suzuki [246]. Recall that we denote by $c_i^{(n)}$ the coefficient of z^i in the n-th cyclotomic polynomial $\Phi_n(z)$, as in formula (8.11).

Theorem 8.7. *For any integer $s \in \mathbb{Z}$, there exists $n, i \in \mathbb{N}$ such that $c_i^{(n)} = s$.*

The result above can be rephrased as follows: every integer can be found among the coefficients of some cyclotomic polynomial. Based on [246], in the proof of this theorem we will make us of the following consequence of the Prime number theorem. We refer to [209] for the full statement and proof.

Proposition 8.2. *Let $t > 2$ be any integer. Then there exist t distinct primes $p_1 < p_2 < \cdots < p_t$ such that $p_1 + p_2 > p_t$.*

Proof. Indeed, suppose the conclusion of the proposition is false for some $t > 2$. Then for any distinct primes $p_1 < p_2 < \cdots < p_t$ we should have that $p_1 + p_2 \leq p_t$. In particular, this implies that $2p_1 < p_t$. As a consequence, we obtain that for any integer $k \geq 2$ the number of primes between 2^{k-1} and 2^k is strictly less than t. If π denotes the prime-counting function, it follows that for every $k \geq t$ we have that $\pi(2^k) = kt$, which gives a contradiction to the Prime Number Theorem. The latter asserts that $\pi(2^k)$ is of the order $\frac{2^k}{k \log 2}$, when $k \to \infty$.

Let us now return to the proof of the Theorem 8.7. Let $t > 2$ be any odd integer. From the proposition above, we know that there are primes $p_1 < p_2 < \cdots < p_t$ such that $p_1 + p_2 > p_t$. We will write shortly $p = p_t$ and $n = p_1 p_2 \cdots p_t$ for the product of all these primes. We will look at the n-th cyclotomic polynomial $\Phi_n(z)$.

Following an earlier idea of Schur, the Suzuki Theorem considers the cyclotomic polinomial $\Phi_n(z)$ modulo z^{p+1}. We have

$$\begin{aligned}\Phi_n(z) &= \prod_{i=1}^{t}(1 - z^{p_i})/(1 - z) \pmod{z^{p+1}} \\ &= (1 + z + \cdots + z^p)(1 - z^{p_1} - \cdots - z^{p_t}) \pmod{z^{p+1}}.\end{aligned}$$

By this formula we deduce that that $c_p^{(n)} = -t + 1$ and $c_{p-2}^{(n)} = -t + 2$. Because t takes every odd positive values greater or equal than 3, this shows that all the integers in the set $\{s \in \mathbb{Z} : s \leq -1\}$ can be found among the coefficients of cyclotomic polynomials.

It is known that for any odd positive integer m, we have the identity $\Phi_{2m}(z) = \Phi_m(-z)$. As for $p_1 \geq 3$, the product $n = p_1 p_2 \cdots p_n$ is odd, this implies that for the above n we have $c_p^{(2n)} = t - 1$ and $c_{p-2}^{(2n)} = t - 2$ which implies that also the integers in the set $\{s \in \mathbb{Z} : s \geq 1\}$ can be found among coefficients of cyclotomic polynomials.

We noted earlier in this chapter that $0 = c_1^{(4)}$, which end the proof. □

Given an integer $|k| \geq 2$, an interesting follow-up problem consists of finding the minimal m for which there exists an n such that $c_m^{(n)} = k$. The problem was first considered in 1991 by Grytezuk and Tropak [121], and here we describe some of the progress made on this, following [250].

If m is such a natural number, then for all n, we must have $c_r^{(n)} \neq k$ for all $r < m$. Taking for instance $k = -2$, it is known that $m = 7$ is minimal and $c_7^{(105)} = -2$. Recall in (8.13) we deduced that

$$\Phi_n(z) = \prod_{d|n} \left(1 - z^d\right)^{\mu(n/d)},$$

where μ is the Möbius function. By setting $\mu(n/d) = 0$ whenever n/d is not an integer, we can write

$$\Phi_n(z) = \prod_{d=1}^{\infty} \left(1 - z^d\right)^{\mu(n/d)}. \tag{8.15}$$

Hence, for a square-free n, the value $c_m^{(n)}$ depends only on the values of $\mu(n)$, $\mu(n/d)$ and on the primes that are less that $m+1$ and divide n.

The following interesting result was proved by Endo [107], who used mathematical induction ande earlier results by Bloom [72] and Erdös [110]). We here provide a direct proof and some simplifications. Then we will formulate a counterpart for the inverse cyclotomic polynomials.

Theorem 8.8. *The following formula holds*

$$c_m^{(n)} = \sum_{i_1+2i_2+\cdots+mi_m=m} (-1)^{i_1+\cdots+i_m} \binom{\mu(n)}{i_1} \binom{\mu(n/2)}{i_2} \cdots \binom{\mu(n/m)}{i_m}, \tag{8.16}$$

where $(i_1,\ldots,i_m)$ runs over all the non-negative integral solutions of the equation $i_1 + 2i_2 + \cdots + mi_m = m$, for m a positive integer.

Proof. We write the infinite product formula (8.15), as

$$\sum_{m=0}^{\infty} \left(\sum_{i_1+2i_2+\cdots+mi_m=m} (-1)^{i_1+\cdots+i_m} \binom{\mu(n)}{i_1} \binom{\mu(n/2)}{i_2} \cdots \binom{\mu(n/m)}{i_m} \right) z^m,$$

and identify the coefficients of z^m. □

By formula (8.16) if we fix m, we can obtain the first coefficients as follows:

- For $m = 1$ the equation $i_1 = 1$ has the solutions $i_1 = 1$, so one obtains

$$c_1^{(n)} = -\mu(n). \tag{8.17}$$

- For $m = 2$ the equation $i_1 + 2i_2 = 2$ has the solutions $(i_1,i_2) = (2,0)$ and $(i_1,i_2) = (0,1)$. Hence, once obtains

$$c_2^{(n)} = \sum_{i_1+2i_2=2} (-1)^{i_1+i_2} \binom{\mu(n)}{i_1} \binom{\mu(n/2)}{i_2} = \binom{\mu(n)}{2} - \binom{\mu(n/2)}{1}$$
$$= \frac{1}{2}\mu(n)\,(\mu(n)-1) - \mu(n/2). \tag{8.18}$$

- For $m = 3$ the solutions of the equation $i_1 + 2i_2 + 3i_3 = 3$ are $(i_1,i_2,i_3) = (3,0,0)$, $(i_1,i_2,i_3) = (1,1,0)$ and $(i_1,i_2,i_3) = (0,0,1)$. This gives

$$\begin{aligned} c_3^{(n)} &= \sum_{i_1+2i_2+3i_3=3} (-1)^{i_1+i_2+i_3} \binom{\mu(n)}{i_1} \binom{\mu(n/2)}{i_2} \binom{\mu(n/3)}{i_3} \\ &= -\binom{\mu(n)}{3} + \binom{\mu(n)}{1}\binom{\mu(n/2)}{1} - \binom{\mu(n/3)}{1} \\ &= -\frac{\mu(n)\,(\mu(n)-1)\,(\mu(n)-2)}{6} + \mu(n)\mu(n/2) - \mu(n/3) \\ &= -\frac{\mu(n)^3 - 3\mu(n)^2 + 2\mu(n)}{6} + \mu(n)\mu(n/2) - \mu(n/3) \\ &= \frac{\mu(n)^2 - \mu(n)}{2} + \mu(n)\mu(n/2) - \mu(n/3), \end{aligned} \tag{8.19}$$

  where we used that $\mu(n)^3 = \mu(n)$, leading to $\binom{\mu(n)}{2} = -\binom{\mu(n)}{3}$.
- For $m = 4$ the solutions (i_1,i_2,i_3,i_4) of equation $i_1 + 2i_2 + 3i_3 + 4i_4 = 4$ are $(0,0,0,1)$, $(1,0,1,0)$, $(0,2,0,0)$, $(2,1,0,0)$, and $(4,0,0,0)$. This gives

$$\begin{aligned} c_4^{(n)} &= \sum_{i_1+2i_2+3i_3+4i_4=4} (-1)^{i_1+\cdots+i_4} \binom{\mu(n)}{i_1} \binom{\mu(n/2)}{i_2} \binom{\mu(n/3)}{i_3} \binom{\mu(n/4)}{i_4} \\ &= \binom{\mu(n)}{4} - \binom{\mu(n)}{2}\mu(n/2) + \binom{\mu(n/2)}{2} + \mu(n)\mu(n/3) - \mu(n/4) \\ &= \frac{\mu(n)^2 - \mu(n)}{2}\,(1 - \mu(n/2)) + \frac{\mu(n/2)^2 - \mu(n/2)}{2} \\ &\quad + \mu(n)\mu(n/3) - \mu(n/4), \end{aligned} \tag{8.20}$$

  where we used that $\mu(n)^3 = \mu(n)$.

The results below helps to simplify calculations in Endo's Theorem 8.16.

Lemma 8.2. *Let $(K,+,\cdot)$ be a a field such that* $\operatorname{char} K = 0$*, and $x \in K$ an element for which $x^3 = x$. If $k \geq 2$ is an integer, then the following identity holds*

$$\binom{x}{k} = (-1)^k \binom{x}{2}, \tag{8.21}$$

where $\binom{x}{k} = \dfrac{x\,(x-1)\cdots(x-k+1)}{k!}$ is a formal binomial coefficient.

Proof. Since $x^3 - x = 0$, the following relations hold

$$\begin{aligned}\binom{x}{k} + \binom{x}{k+1} &= \frac{x(x-1)\cdots(x-k+1)}{k!} \\ &\quad + \frac{x(x-1)\cdots(x-k+1)(x-k)}{(k+1)!} \\ &= \frac{x(x-1)\cdots(x-k+1)}{(k+1)!} \cdot (k+1+x-k) \\ &= (x+1)\,x\,(x-1)\,\frac{\prod_{j=3}^{k}(x-j+1)}{(k+1)!} = 0.\end{aligned}$$

This identity shows that $\binom{x}{k+1} = -\binom{x}{k}$, for $k \geq 0$, hence

$$\binom{x}{2} = -\binom{x}{3} = \binom{x}{4} = \cdots = (-1)^k \binom{x}{k},$$

confirming the desired identity for $k \geq 2$. □

As a consequence, since $\mu(n) \in \{-1, 0, 1\}$ $(n \geq 1)$, ensures that $\mu(n)^3 = \mu(n)$, for an integer $k \geq 2$ we have

$$\binom{\mu(n)}{k} = (-1)^k \binom{\mu(n)}{2}. \tag{8.22}$$

Therefore, if $(i_1, \ldots, i_m)$ is a solution of the equation $i_1 + 2i_2 + \cdots + mi_m = m$ and for a given $j = 1, \ldots, m$ the corresponding index satisfies $i_j \geq 2$, then the corresponding binomial coefficient in (8.16) having the form $(-1)^{i_j}\binom{\mu(n/j)}{i_j}$, can be replaced using formula (8.22) by $\binom{\mu(n/j)}{2}$. For example, this allows quicker calculations for $c_3^{(n)}$ in (8.19) and $c_4^{(n)}$ in (8.20). Splitting the indices of a fixed vector $(i_1, \ldots, i_m)$ solution to $i_1 + 2i_2 + \cdots + mi_m = m$ into two sets

$$J_1 = \{j \in 1, \ldots, m \mid i_j = 1\}, \quad J_2 = \{j \in 1, \ldots, m \mid i_j \geq 2\},$$

the corresponding term in Endo's formula can be rewritten as

$$\begin{aligned}&(-1)^{i_1+\cdots+i_m}\binom{\mu(n)}{i_1}\binom{\mu(n/2)}{i_2}\cdots\binom{\mu(n/m)}{i_m} \\ &= (-1)^{|I_1|} \cdot \prod_{j\in J_1} \mu(n/j) \cdot \prod_{j\in J_2} \binom{\mu(n/j)}{2}.\end{aligned} \tag{8.23}$$

We first find upper bounds for selected coefficients.

Example 8.17. *Let us confirm that* $|c_2^{(n)}| \leq 1$.

Solution. Indeed, by the Theorem, and formula (8.18), when $\mu(n) = 0$ or 1, $\frac{1}{2}\mu(n)\left(\mu(n)-1\right) = 0$, hence $c_2 = -\mu\left(n/2\right)$. On the other hand, when $\mu(n) = -1$, one obtains $1/2\mu(n)\left(\mu(n)-1\right) = 1$. Clearly, if the number $n/2$ is an integer, then $\mu(n/2) = 1$, hence $c_2 = 0$. On the other hand, when $n/2$ is not an integer, we gave $\mu(n/2) = 0$, in which case $c_2 = 1$. One can observe that in all cases $|c_2^{(n)}| \leq 1$.

Similar calculations can be used to prove that $|c_m^{(n)}| \leq 1$ for $m = 3,\ldots,6$. Below we detail the computations for $m = 7$.

Example 8.18. *Let us prove that* $|c_7^{(n)}| \leq 2$.

Solution. We analyse all configurations for which $i_1 + 2i_2 + \cdots + 7i_7 = 7$ and the formula below :

$$c_7^{(n)} = \sum_{i_1+2i_2+\cdots+7i_7=7} (-1)^{i_1+\cdots+i_7} \binom{\mu(n)}{i_1} \binom{\mu(n/2)}{i_2} \cdots \binom{\mu(n/7)}{i_7}. \quad (8.24)$$

Using this approach it is proved that

(I). $c_7^{(n)} = -2$ for $\mu(n) = 1$ and n divisible by $2 \times 3 \times 5 \times 7$;
(II). $c_7^{(n)} = 2$ when $\mu(n) = -1$, for n odd and divisible by $3 \times 5 \times 7$;
(III). $|c_7^{(n)}| \leq 1$ otherwise.

Indeed, the details of these cases are discussed below.
Case (I). For $\mu(n) = 0$, one has $\binom{\mu(n)}{i_1}$ for $i_1 \geq 1$, hence

$$c_7^{(n)} = \sum_{2i_2+\cdots+7i_7=7} (-1)^{i_2+\cdots+i_7} \binom{\mu(n/2)}{i_2} \cdots \binom{\mu(n/7)}{i_7},$$

while the equation $2i_2 + \cdots + 7i_7 = 7$ has only the four solutions

$$i_2 = 2, i_3 = 1; \quad i_2 = 1, i_5 = 1; \quad i_3 = 1, i_4 = 1; \quad i_7 = 1,$$

where the numbers not explicitly mentioned are zero.

It follows that

$$c_7^{(n)} = -\frac{1}{2}\mu\left(n/2\right)\left(\mu\left(n/2\right)-1\right)\mu\left(n/3\right) + \mu\left(n/2\right)\mu\left(n/5\right) + \mu\left(n/3\right)\mu\left(n/4\right) - \mu\left(n/7\right).$$

Here we have three scenarios.
(I-a). If $\mu(n/2) = 1$, then n is a multiple of 4, which implies that we have $\mu(n/3) = \mu(n/5) = \mu(n/7) = 0$, hence $c_7 = 0$.
(I-b). If $\mu(n/2) = 0$ and $p^2 \mid n$ with $p \neq 7$ and $7^3 \mid n$, then

$$c_7^{(n)} = \mu\left(n/3\right)\mu\left(n/4\right) - \mu\left(n/7\right).$$

If $\mu(n/2) = 0$ and $7^2 \mid n$, then

$$c_7^{(n)} = -\mu\,(n/7)\,.$$

(I-c). If $\mu(n/2) = -1$, then n must be a multiple of 4 and so we have $\mu(n/3) = \mu(n/5) = \mu(n/7) = 0$, hence $c_7 = 0$.

Case (II). When $\mu(n) = 1$, we have $\binom{\mu(n)}{i_1} = 0$ for $i_1 \geq 2$, and as $\mu(n/4) = 1$

$$\begin{aligned} c_7^{(n)} = {} & \mu\,(n)\,\frac{1}{6}\mu\,(n/2)\,(\mu\,(n/2)-1)\,(\mu\,(n/2)-2) \\ & - \mu\,(n)\,\frac{1}{2}\mu\,(n/3)\,(\mu\,(n/3)-1) + \mu\,(n)\,\mu\,(n/6) \\ & - \frac{1}{2}\mu\,(n/2)\,(\mu\,(n/2)-1)\,\mu\,(n/3) + \mu\,(n/2)\,\mu\,(n/5) - \mu\,(n/7)\,. \end{aligned}$$

(IIa). If n is not even, then $\mu(n/2) = 0$, therefore

$$c_7^{(n)} = -\frac{1}{2}\mu\,(n/3)\,(\mu\,(n/3)-1) - \mu\,(n/7)\,,$$

where $\mu(n) = 1$, while $-\mu(n/7) = 1$ or 0, if $7 \mid n$ or not. Also, we have

$$-\frac{1}{2}\mu\,(n/3)\,(\mu\,(n/3)-1) = -1 \text{ or } 0,$$

if $3 \mid n$ or not, hence $|c_7| \leq 1$.

(II-b). If n is a multiple of 2, then $\mu\,(n/2) = -1$, hence

$$\begin{aligned} c_7^{(n)} = {} & -1 - \frac{1}{2}\mu\,(n/3)\,(\mu\,(n/3)-1) \\ & + \mu\,(n/6) - \mu\,(n/3) - \mu\,(n/5) - \mu\,(n/7)\,. \end{aligned}$$

(II-b-1). If n is not multiple of 3, then $\mu\,(n/3) = 0$, so we have

$$c_7^{(n)} = -1 - \mu\,(n/5) - \mu\,(n/7)\,.$$

Since $\mu(n) = 1$ and $\mu\,(n/5)$, $\mu\,(n/7)$ are -1 or 0, it follows that $|c_7| \leq 1$.

(II-b-2). If $3 \mid n$ then $\mu\,(n/3) = -1$ so that $\mu\,(n/6) = 1$, hence

$$c_7^{(n)} = -1 - 1 + 1 + 1 - \mu\,(n/5) - \mu\,(n/7)\,.$$

In this case if $5 \mid n$ and $7 \mid n$ then $|c_7| = 2$. For example, this can be checked for $n = 2 \times 3 \times 5 \times 7 = 210$, where $c_7 = 2$.

We now move to the final case.

Case (III). When $\mu(n) = -1$, $\binom{\mu(n)}{i_1} = (-1)^{i_1}$ and $\mu(n/4) = 0$ since $n/4$ is not an integer. Hence the following formula is obtained:

$$c_7^{(n)} = 1 - \mu(n/2) - \mu(n/3) + \frac{1}{2}\mu(n/2)(\mu(n/2) - 1) + \mu(n/2)\mu(n/3)$$
$$- \mu(n/5) - \frac{1}{6}\mu(n/2)(\mu(n/2) - 1)(\mu(n/2) - 2) + \frac{1}{2}\mu(n/3)(\mu(n/3) - 1)$$
$$- \mu(n/6) - \frac{1}{2}\mu(n/2)(\mu(n/2) - 1)\mu(n/3) + \mu(n/2)\mu(n/5) - \mu(n/7).$$

Since $\mu(n) = -1$, with $\mu(n/2)$ and $\mu(n/3)$ being 1 or 0, the formula becomes

$$c_7^{(n)} = (1 - \mu(n/2))(1 - \mu(n/3)) - \mu(n/5) - \mu(n/6)$$
$$+ \mu(n/2)\mu(n/5) - \mu(n/7).$$

(III-a). If $\mu(n/2) = 1$ one has

$$c_7^{(n)} = -\mu(n/6) - \mu(n/7).$$

Since $\mu(n/2) = 1$, we get $\mu(n) = 0$ or -1. Also $\mu(n/7) = 0$ or 1, so $|c_7| \leq 1$.

(III-b). If $\mu(n/2) = 0$ then $\mu(n/6) = 0$ and

$$c_7^{(n)} = 1 - \mu(n/3) - \mu(n/5) - \mu(n/7).$$

Hence, if $\mu(n/3) = \mu(n/5) = \mu(n/7) = 1$, in which case $c_7 = -2$. One can check that for $n = 3 \times 5 \times 7 = 105$ one has $c_7 = -2$.

In the same paper it is mentioned that $|c_8^{(n)}| \leq 2$ and $|c_9^{(n)}| \leq 2$.

In the aforementioned article [121], Grytezuk and Tropak derived the following recurrence relation for these coefficients. First, observe that $c_0^{(n)} = 1$.

Then, for $m \geq 2$ we have

$$c_m^{(n)} = -\frac{\mu(n)}{m} \sum_{l=0}^{m-1} \mu(\gcd(n, m-l))\varphi(\gcd(n, m-l))c_l^{(n)}, \tag{8.25}$$

where φ denotes the Euler's totient function.

We note the following interesting connection between the coefficients of cyclotomic polynomials and Ramanujan sums.

Let $c_j^{(n)}$ be the coefficient of z^j in the n-th cyclotomic polynomial. We first recall that the cyclotomic polynomials are reciprocal. Moreover, for every $1 \leq j \leq \varphi(n) - 1$, using Viéta's formula one can write $c_j^{(n)} = c_{\varphi(n)-j}^{(n)}$ the evaluation of the symmetric polynomial S_j in the primitive n-th roots of unity.

On the other hand, the Ramanujan sums $\rho(n,k)$ are just the evaluation of the symmetric polynomial P_k in the primitive n-th roots of unity.

Newton's identities discussed previously, assert that the polynomials $S_1,\ldots,S_{\varphi(q)}$ and $P_1,P_2,\ldots,P_{\varphi(n)}$ are related by the following relations

$$P_k - S_1P_{k-1} + S_2P_{k-2} - \cdots + (-1)^{k-1}S_{k-1}P_1 + (-1)^k kS_k = 0,$$

which hold for every $k \in \{2,\ldots,\varphi(n)\}$.

This leads to an interesting recursive formula.

Theorem 8.9. *The following identities hold for every k in the aforementioned set:*

$$c_k^{(n)} = -\frac{1}{k}\left[\rho(n,k) + \rho(n,k-1)c_1^{(n)} + \cdots + \rho(n,1)c_{k-1}^{(n)}\right]. \tag{8.26}$$

We apply the above recurrence relation to compute the first four coefficients $c_k^{(n)}$, for every $n \in \mathbb{N}^*$ as follows:

- For $k = 1$ one obtains

$$c_1^{(n)} = -\rho(n,1) = -\mu(n).$$

- For $k = 2$ we have

$$\begin{aligned} c_2^{(n)} &= -\frac{1}{2}\left[\rho(n,2) + \rho(n,1)c_1^{(n)}\right] \\ &= -\frac{1}{2}\left[\mu(n) + 2\mu\left(n/2\right) - \mu(n)^2\right] \\ &= \frac{\mu(n)^2 - \mu(n)}{2} - \mu\left(n/2\right). \end{aligned}$$

- For $k = 3$, using the identity $\mu(n)^3 = \mu(n)$ one obtains

$$\begin{aligned} c_3^{(n)} &= -\frac{1}{3}\left[\rho(n,3) + \rho(n,2)c_1^{(n)} + \rho(n,1)c_2^{(n)}\right] \\ &= -\frac{\mu(n) + 3\mu(n/3)}{3} + \frac{\mu(n) + 2\mu(n/2)}{3}\mu(n) - \\ &\quad - \mu(n)\left(\frac{\mu(n)^2 - \mu(n)}{6} - \frac{\mu(n/2)}{3}\right) \\ &= \frac{\mu(n)^2 - \mu(n)}{2} + \mu(n)\mu(n/2) - \mu(n/3). \end{aligned}$$

- For $k = 4$ since $\mu(n)^3 = \mu(n)$ and $\mu(n)^4 = \mu(n)^2$ we confirm that

$$\begin{aligned}
c_4^{(n)} &= -\frac{1}{4}\left[\rho(n,4)+\rho(n,3)c_1^{(n)}+\rho(n,2)c_2^{(n)}+\rho(n,1)c_3^{(n)}\right] \\
&= -\frac{\mu(n)+2\mu(n/2)+4\mu(n/4)}{4}+\frac{\mu(n)+3\mu(n/3)}{4}\mu(n) \\
&- \frac{\mu(n)+2\mu(n/2)}{4}\left(\frac{\mu(n)^2-\mu(n)}{2}-\mu(n/2)\right) \\
&- \left(\frac{\mu(n)^2-\mu(n)}{8}+\frac{\mu(n)\mu(n/2)}{4}-\frac{\mu(n/3)}{4}\right)\mu(n) \\
&= \frac{\mu(n)^2-\mu(n)}{2}\left(1-\mu(n/2)\right)+\frac{\mu(n/2)^2-\mu(n/2)}{2} \\
&+ \mu(n)\mu(n/3)-\mu(n/4).
\end{aligned}$$

The relation (8.26) suggests that every coefficient $c_k^{(n)}$ of the n-th cyclotomic polynomial is a polynomial with rational coefficients in the variables $\rho(n,k)$, $k=1,2,\ldots,\varphi(n)-1$ given by Ramanujan sums. The explicit form of this polynomial is given in the following result, linked to Theorem 7.3.

Theorem 8.10. *We have*

$$c_k^{(n)} = \sum_{l_1+2l_2+\cdots+kl_k=k} (-1)^{l_1+l_2+\cdots+l_k}\frac{\rho(n,1)^{l_1}}{1^{l_1}l_1!}\cdot\frac{\rho(n,2)^{l_2}}{2^{l_2}l_2!}\cdot\ldots\cdot\frac{\rho(n,k)^{l_k}}{k^{l_k}l_k!}. \quad (8.27)$$

As direct corollaries of the above, we can recover the formulas for the first four cyclotomic coefficients as follows:

- For $k=1$, the equation $l_1=1$ has the (only) solution $l_1=1$, hence

$$c_1^{(n)} = -\rho(n,1) = -\mu(n).$$

- For $k=2$, the equation $l_1+2l_2=2$ has the solutions $(l_1,l_2)=(2,0)$ and $(l_1,l_2)=(0,1)$. We therefore get

$$\begin{aligned}
c_2 &= \frac{1}{2}\rho(n,1)^2-\frac{1}{2}\rho(n,2) = \frac{1}{2}\mu^2(n)-\frac{1}{2}\left(\mu(n)+2\mu(n/2)\right) \\
&= \frac{\mu(n)^2-\mu(n)}{2}-\mu(n/2).
\end{aligned}$$

  Recall that $\mu(n)^3=\mu(n)$ for every $n\in\mathbb{N}^*$ and using this identity one can simplify the expressions involving powers of the Möbius function.

- For $k=3$ the solutions (l_1,l_2,l_3) of the equation $l_1+2l_2+3l_3=3$ are $(3,0,0)$, $(1,1,0)$ and $(0,0,1)$, therefore

$$c_3^{(n)} = -\frac{1}{6}\rho^3(n,1) + \frac{1}{2}\rho(n,1)\rho(n,2) - \frac{1}{3}\rho(n,3)$$
$$= -\frac{1}{6}\mu^3(n) + \frac{1}{2}\mu(n)\left(\mu(n) + 2\mu\left(\frac{n}{2}\right)\right) - \frac{1}{3}\left(\mu(n) + 3\mu\left(n/3\right)\right)$$
$$= \frac{\mu(n)^2 - \mu(n)}{2} + \mu(n)\mu\left(n/2\right) - \mu\left(n/3\right).$$

- For $k = 4$, the solutions (l_1, l_2, l_3, l_4) of the equation $l_1 + 2l_2 + 3l_3 + 4l_4 = 4$ are $(4,0,0,0)$, $(2,1,0,0)$, $(0,2,0,0)$, $(1,0,1,0)$, $(0,0,0,1)$, hence

$$c_4^{(n)} = \frac{\rho(n,1)^4}{24} - \frac{1}{4}\rho(n,1)^2\rho(n,2) + \frac{1}{8}\rho^2(n,2) + \frac{1}{3}\rho(n,1)\rho(n,3) - \frac{1}{4}\rho(n,4)$$
$$= \frac{1}{24}\mu^4(n) - \frac{1}{4}\mu^2(n)\left(\mu(n) + 2\mu\left(n/2\right)\right) + \frac{1}{8}\left(\mu(n) + 2\mu\left(n/2\right)\right)^2$$
$$+ \frac{1}{3}\mu(n)\left(\mu(n) + 3\mu\left(n/3\right)\right) - \frac{1}{4}\left(\mu(n) + 2\mu\left(n/2\right) + 4\mu\left(\frac{n}{4}\right)\right)$$
$$= \frac{\mu(n)^2 - \mu(n)}{2}\left(1 - \mu(n/2)\right) + \frac{\mu(n/2)^2 - \mu(n/2)}{2}$$
$$+ \mu(n)\mu(n/3) - \mu(n/4).$$

Using the identity $\mu^3 = \mu$ in Theorem 8.8, we obtain a useful result.

Corollary 8.4. *For every $n \in \mathbb{N}^*$ and every $k \in \{1,2,\ldots,\varphi(n)\}$, the cyclotomic coefficient $c_k^{(n)}$ is a polynomial with rational coefficients in $\mu(n/d)$, where d is a divisor of n. Moreover, the degree of $\mu(n/d)$ in every monomial is at most 2.*

8.6 The integral formula for the coefficients of Φ_n

Explicit formulae calculations for the coefficients are mentioned in [229, p.258-259], and involve complicated expressions. Using Stirling and Bernoulli numbers, [181] has obtained formulae for the coefficients of $\Phi_n(z+1)$ as polynomials with rational coefficients of certain Jordan functions.

Integer sequences related to the coefficients of cyclotomic polynomials can be found in the Online Encyclopedia of Integer Sequences [211].

In this section we use derive an integral formula for the coefficients of Φ_n, then discuss some applications, related to the direct and alternate sums of coefficients, along with a formula for the mid-term of Φ_n. Integral formulae for the coefficients were derived by Andrica and Bagdasar in [20].

8.6.1 The integral formula

The proof a known identity involving Euler's totient function.

Lemma 8.3. *Let $n \geq 3$ be a positive integer. The following formula holds:*

$$\sum_{\substack{1\leq k\leq n-1\\ \gcd(k,n)=1}} k = \frac{n}{2}\varphi(n). \tag{8.28}$$

Proof. If $k \in \{1,\dots,n-1\}$ is relatively prime with n, then so is number $n-k$. There are $\varphi(n)$ numbers relatively prime with n in total, hence there are $\varphi(n)/2$ pairs of numbers which sum up to n. □

In order to get a unitary formula for $c_j^{(n)}$, we introduce the function

$$\Lambda_n(t) = \prod_{\substack{1\leq k\leq n-1\\ \gcd(k,n)=1}} \sin\left(t - \frac{k\pi}{n}\right). \tag{8.29}$$

For $n = 1,2$ one obtains the following expressions:

$$\Lambda_1(t) = \sin(t-\pi) = -\sin t,$$
$$\Lambda_2(t) = \sin\left(t - \frac{\pi}{2}\right) = -\cos t.$$

For the first few values $n = 3,4,5,6$ we have

$$\Lambda_3(t) = \sin\left(t-\frac{\pi}{3}\right)\sin\left(t-\frac{2\pi}{3}\right) = \frac{1}{2}\cos 2t + \frac{1}{4}.$$
$$\Lambda_4(t) = \sin\left(t-\frac{\pi}{4}\right)\sin\left(t-\frac{3\pi}{4}\right) = \frac{1}{2}\cos 2t.$$
$$\Lambda_5(t) = \sin\left(t-\frac{\pi}{5}\right)\sin\left(t-\frac{2\pi}{5}\right)\sin\left(t-\frac{3\pi}{5}\right)\sin\left(t-\frac{4\pi}{5}\right)$$
$$= \frac{1}{16}\left(2\cos 2t + 2\cos 4t + 1\right).$$
$$\Lambda_6(t) = \sin\left(t-\frac{2\pi}{6}\right)\sin\left(t-\frac{5\pi}{6}\right) = \frac{1}{2}\cos 2t - \frac{1}{4}.$$

As polynomials $\Phi_1(z)$ and $\Phi_2(z)$ are linear, we may assume $n \geq 3$.

Theorem 8.11. *The coefficients $c_j^{(n)}$ are given by the following integral formula:*

$$c_j^{(n)} = \frac{2^{\varphi(n)}}{\pi}\int_0^\pi \Lambda_n(t)\cdot\cos(\varphi(n)-2j)t\,\mathrm{d}t, \quad j = 0,1,\dots,\varphi(n). \tag{8.30}$$

Proof. Denote by $\zeta_n = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$ and let $z = \cos 2t + i\sin 2t$, $t \in [0, 2\pi]$.

By the well-known de Moivre formula and work with complex numbers in polar form (see for example [6]), for $k = 1, \ldots, n$, we have

$$\begin{aligned} z - \zeta_n^k &= \left(\cos 2t - \cos\frac{2k\pi}{n}\right) + i\left(\sin 2t - \sin\frac{2k\pi}{n}\right) \\ &= -2\sin\left(t - \frac{k\pi}{n}\right)\sin\left(t + \frac{k\pi}{n}\right) + 2i\sin\left(t - \frac{k\pi}{n}\right)\cos\left(t + \frac{k\pi}{n}\right) \\ &= 2i\sin\left(t - \frac{k\pi}{n}\right)\left[\cos\left(t + \frac{k\pi}{n}\right) + i\sin\left(t + \frac{k\pi}{n}\right)\right]. \end{aligned}$$

By Lemma 8.3, for $n \geq 3$, one can write the polynomial $\Phi_n(z)$ in the form

$$\begin{aligned} \Phi_n(z) &= \prod_{\substack{1\leq k\leq n-1 \\ \gcd(k,n)=1}} (z - \zeta_n^k) \\ &= (2i)^{\varphi(n)} \prod_{\substack{1\leq k\leq n-1 \\ \gcd(k,n)=1}} \sin\left(t - \frac{k\pi}{n}\right)\left[\cos\left(t + \frac{k\pi}{n}\right) + i\sin\left(t + \frac{k\pi}{n}\right)\right] \\ &= (2i)^{\varphi(n)}\Lambda_n(t) \prod_{\substack{1\leq k\leq n-1 \\ \gcd(k,n)=1}} \left[\cos\left(t + \frac{k\pi}{n}\right) + i\sin\left(t + \frac{k\pi}{n}\right)\right] \\ &= (2i)^{\varphi(n)}\Lambda_n(t)\left[\cos\left(\varphi(n)t + \frac{\varphi(n)\pi}{2}\right) + i\sin\left(\varphi(n)t + \frac{\varphi(n)\pi}{2}\right)\right] \\ &= (2i)^{\varphi(n)}(-1)^{\frac{\varphi(n)}{2}}\Lambda_n(t)\left[\cos\varphi(n)t + i\sin\varphi(n)t\right] \\ &= 2^{\varphi(n)}\Lambda_n(t)\left[\cos\varphi(n)t + i\sin\varphi(n)t\right]. \end{aligned}$$

where we have used that $\varphi(n)$ is even for $n \geq 3$, and the multiplication of complex numbers in polar form. For every $j = 0, 1, \ldots, \varphi(n)$, one may write

$$\begin{aligned} c_j^{(n)} + \sum_{k\neq j} c_k^{(n)} z^{k-j} &= z^{-j} \prod_{\substack{1\leq k\leq n-1 \\ \gcd(k,n)=1}} (z - \zeta_n^k) \\ &= 2^{\varphi(n)}\Lambda_n(t)\left(\cos 2jt - i\sin 2jt\right)\left[\cos\varphi(n)t + i\sin\varphi(n)t\right] \\ &= 2^{\varphi(n)}\Lambda_n(t)[\cos(\varphi(n) - 2j)t + i\sin(\varphi(n) - 2j)t]. \end{aligned}$$

Integrating on the interval $[0, \pi]$ we obtain formula (8.30). This is true since the integral of z^{k-j} over $[0, \pi]$ vanishes whenever $k \neq j$. □

In addition, from the proof of the integral formula (8.30) it follows that

$$\int_0^\pi \Lambda_n(t)\sin(\varphi(n) - 2j)t\,\mathrm{d}t = 0, \quad j = 0, 1, \ldots, \varphi(n). \tag{8.31}$$

8.6.2 Some applications of the integral formula

The formula in Theorem 8.11 can be used to show that the coefficients of the cyclotomic polynomial are reciprocal, to derive compact formulae for the mid-term of cyclotomic polynomials, as well as for the direct and alternate sums of coefficients. Details of the calculations can be found in [20].

Reciprocity of coefficients. It is known that the cyclotomic polynomial $\Phi_n(z)$ is reciprocal, that is its coefficients satisfy

$$c_j^{(n)} = c_{\varphi(n)-j}^{(n)}, \quad j = 0, 1, \ldots, \varphi(n).$$

Indeed, using formula (8.30), for every $j = 0, 1, \ldots, \varphi(n)$, we have

$$\begin{aligned} c_{\varphi(n)-j}^{(n)} &= \frac{2^{\varphi(n)}}{\pi} \int_0^\pi \Lambda_n(t) \cdot \cos\left(\varphi(n) - 2(\varphi(n) - j)\right) t \, \mathrm{d}t \\ &= \frac{2^{\varphi(n)}}{\pi} \int_0^\pi \Lambda_n(t) \cdot \cos\left(\varphi(n) - 2j\right) t \, \mathrm{d}t = c_j^{(n)}. \end{aligned}$$

Direct sum of coefficients $\Phi_n(1)$. The following explicit formula is known:

$$\Phi_n(1) = \begin{cases} 0 & \text{if } n = 1; \\ p & \text{if } n = p^m; \\ 1 & \text{otherwise,} \end{cases} \tag{8.32}$$

where $m \geq 1$ is an integer and p is prime. This integer sequence is labeled A014963 in [211], has stretches of 1 of arbitrary length, and starts with

$$0, 2, 3, 2, 5, 1, 7, 2, 3, 1, 11, 1, 13, 1, 1, 2, 17, 1, 19, 1, 1, 1, 23, \ldots$$

By the formula (8.30) for the coefficients $c_j^{(n)}$, we obtain an integral equivalent formula $\Phi_n(1)$, valid for $n \geq 3$, as follows:

$$\begin{aligned} \Phi_n(1) &= \sum_{j=0}^{\varphi(n)} c_j^{(n)} \\ &= \sum_{j=0}^{\varphi(n)} \frac{2^{\varphi(n)}}{\pi} \int_0^\pi \Lambda_n(t) \cdot \cos(\varphi(n) - 2j) t \, \mathrm{d}t, \\ &= \frac{2^{\varphi(n)}}{\pi} \int_0^\pi \Lambda_n(t) \cdot \left[\sum_{j=0}^{\varphi(n)} \cos(\varphi(n) - 2j) t \right] \mathrm{d}t \\ &= \frac{2^{\varphi(n)}}{\pi} \int_0^\pi \Lambda_n(t) \frac{\sin(\varphi(n) + 1) t}{\sin t} \, \mathrm{d}t. \end{aligned} \tag{8.33}$$

The integral in (8.33) is not improper. Indeed, by de Moivre's formula

$$\cos(\varphi(n)+1)t + i\sin(\varphi(n)+1)t = (\cos t + i\sin t)^{\varphi(n)+1}.$$

Separating the real and imaginary parts one can show that

$$\cos(\varphi(n)+1)t = \sum_{j=0}^{\varphi(n)/2} \left[(-1)^j \binom{\varphi(n)+1}{2j} (\cos t)^{\varphi(n)-2j} (\sin t)^{2j}\right] \cos t,$$

$$\sin(\varphi(n)+1)t = \sum_{j=0}^{\varphi(n)/2} \left[(-1)^j \binom{\varphi(n)+1}{2j+1} (\cos t)^{\varphi(n)-2j} (\sin t)^{2j}\right] \sin t,$$

hence $\frac{\sin(\varphi(n)+1)t}{\sin t}$ is in fact a polynomial in $\sin t$ and $\cos t$.

Formula (8.33) can also be proved using the sum of cosines:

$$\begin{aligned}
&\sum_{j=0}^{\varphi(n)} \cos(\varphi(n)-2j)t \cdot \sin t \\
&= \sum_{j=0}^{\varphi(n)} \frac{1}{2}\left[\sin(\varphi(n)-2j+1)t - \sin(\varphi(n)-2j-1)t\right] \\
&= \frac{1}{2}\left[\sin(\varphi(n)+1)t - \sin(-\varphi(n)-1)t\right] \\
&= \sin(\varphi(n)+1)t,
\end{aligned}$$

and dividing by $\sin t$.

The mid-term of $\Phi_n(z)$. The middle coefficients obtained for $n \geq 3$ produce the integer sequence A094754 in OEIS, which starts with the terms

$$1,0,1,-1,1,0,1,1,1,-1,1,-1,-1,0,1,-1,1,1,...$$

These are also given by the integral formula

$$m_n = c^{(n)}_{\frac{\varphi(n)}{2}} = \frac{2^{\varphi(n)}}{\pi} \int_0^{\pi} \Lambda_n(t)\,\mathrm{d}t. \tag{8.34}$$

As Φ_n is reciprocal we have $\Phi_n(1) = 2a + m_n$, with a integer. By (8.32), $\Phi_n(1)$ is odd if n is not a power of 2, in which case m_n is also odd. Moreover, $m_n = 0$ if and only if $n = 2^m$ for some $m \geq 2$. By formula (8.34) we obtain

$$\int_0^{\pi} \Lambda_n(t)\,\mathrm{d}t = 0, \quad \text{if and only if } n = 2^m, \quad m \geq 1.$$

While the terms of the sequence m_n seem to be equal to -1, 0 or 1, other negative and positive values appear. For example $m_{385} = -3$, $m_{6545} = -5$ and $m_{7735} = -7$, while $m_{1155} = 3$, $m_{4785} = 5$, and $m_{11305} = 19$. Some of these values are mentioned in the paper of Dresden [103].

This suggests that every odd integer may be the mid-coefficient of some cyclotomic polynomial [20, Conjecture].

Alternate sum of coefficients $\Phi_n(-1)$. The following formula is known

$$\Phi_n(-1) = \begin{cases} -2 & \text{if } n = 1; \\ 0 & \text{if } n = 2; \\ p & \text{if } n = 2p^m; \\ 1 & \text{otherwise,} \end{cases} \tag{8.35}$$

where $m \geq 1$ is an integer. This is sequence A020513 in OEIS and starts with

$$-2,0,1,2,1,3,1,2,1,5,1,1,1,7,1,2,1,3,1,1,1,11,1,1,1,13,\ldots.$$

From the formula (8.30) for the coefficients $c_j^{(n)}$, we obtain an integral equivalent formula $\Phi_n(-1)$, valid for $n \geq 3$, as follows.

$$\begin{aligned} \Phi_n(-1) = \sum_{j=0}^{\varphi(n)} c_j^{(n)}(-1)^j &= \sum_{j=0}^{\varphi(n)} \frac{2^{\varphi(n)}}{\pi} \int_0^\pi \Lambda_n(t)(-1)^j \cos(\varphi(n)-2j)t \, \mathrm{d}t, \\ &= \frac{2^{\varphi(n)}}{\pi} \int_0^\pi \Lambda_n(t) \left[\sum_{j=0}^{\varphi(n)} (-1)^j \cos(\varphi(n)-2j)t \right] \mathrm{d}t \\ &= \frac{2^{\varphi(n)}}{\pi} \int_0^\pi \Lambda_n(t) \frac{\cos(\varphi(n)+1)t}{\cos t} \, \mathrm{d}t. \end{aligned} \tag{8.36}$$

To prove the last identity we note that for a fixed $j \in \{0,\ldots,\varphi(n)\}$, one has

$$(-1)^j \cos(\varphi(n)-2j)t = \cos\left[(\varphi(n)-2j)t - j\pi\right] = \cos\left[\varphi(n)t - 2j\left(t+\frac{\pi}{2}\right)\right].$$

One can multiply this last expression by $\sin\left(t+\frac{\pi}{2}\right)$ and add the terms $\cos\left[\varphi(n)t - 2j\left(t+\frac{\pi}{2}\right)\right] \cdot \sin\left(t+\frac{\pi}{2}\right)$, $j = 0,\ldots,\varphi(n)$. Using the simple identities $\sin(x+\pi/2) = \cos x$, $\cos(x+k\pi) = (-1)^k \cos x$, $k \in \mathbb{Z}$ one obtains

$$\begin{aligned} \sum_{j=0}^{\varphi(n)} (-1)^j \cos(\varphi(n)-2j)t &= \frac{\cos(\varphi(n)+1)t}{\cos t} \cdot \frac{1+(-1)^{\varphi(n)}}{2} \\ &= \frac{\cos(\varphi(n)+1)t}{\cos t}, \end{aligned}$$

since $\varphi(n)$ is even for $n \geq 3$.

8.7 The inverse cyclotomic polynomial

In this section we discuss properties of a family of polynomials which are closely related to the cyclotomic polynomials.

Definition 8.3 ([204]). For an integer $n \geq 2$, the n-th inverse cyclotomic polynomial $\Psi_n(z)$ is defined by

$$\Psi_n(z) = \prod_{1 \leq k < n, \gcd(k,n) > 1} \left(z - e^{\frac{2k\pi i}{n}} \right) = \frac{x^n - 1}{\Phi_n(z)} = \sum_{j=0}^{n-\varphi(n)} d_j^{(n)} z^j.$$

The roots of this monic polynomial are the non-primitive nth roots of unity, and the degree is $n - \varphi(n)$.

To fix the notation, from now on we will write $d_j^{(n)}$ for the coefficient of z^j in the n-th inverse cyclotomic polynomial Ψ_n, where $\deg \Psi_n = n - \varphi(n)$.

The first inverse cyclotomic polynomials (discounting prime indices) are

$$\begin{aligned}
&\Psi_1(z) = 1,\ \Psi_4(z) = z^2 - 1,\ \Psi_6(z) = z^4 + z^3 - z - 1,\ \Psi_8(z) = z^4 - 1,\\
&\Psi_9(z) = z^3 - 1,\ \Psi_{10}(z) = z^6 + z^5 - z - 1,\ \Psi_{12}(z) = z^8 + z^6 - z^2 - 1,\\
&\Psi_{14}(z) = z^8 + z^7 - z - 1,\ \Psi_{15}(z) = z^7 + z^6 + z^5 - z^2 - z - 1,\\
&\Psi_{16}(z) = z^8 - 1,\ \Psi_{18}(z) = z^{12} + z^9 - z^3 - 1,\ \Psi_{20}(z) = z^{12} + z^{10} - z^2 - 1,\\
&\Psi_{21}(z) = z^9 + z^8 + z^7 - z^2 - z - 1,\ \Psi_{22}(z) = z^{12} + z^{11} - z^2 - 1.
\end{aligned}$$

Proposition 8.3. *The following properties hold:*

1° *If p is a prime and $n = p^\alpha$ for $\alpha \geq 1$ then $\Psi_n(z) = z^{p^{\alpha-1}} - 1$.*
2° *For $n = p_1 \cdots p_k$ square-free, $\deg(\Psi_n) = p_1 \cdots p_k - (p_1 - 1) \cdots (p_k - 1)$.*
3° *If $p < q$ are primes, then for $n = pq$ one has*

$$\Psi_n(z) = \frac{(z^p - 1)(z^q - 1)}{z - 1} = z^{p+q-1} + \cdots + z^{q+1} - z^{p-1} - \cdots - z^2 - z - 1.$$

4° *If p, q, r are different primes, then for $n = pqr$ one has*

$$\Psi_n(z) = \frac{(z^{pq} - 1)(z^{qr} - 1)(z^{rp} - 1)(z - 1)}{(z^p - 1)(z^q - 1)(z^r - 1)}.$$

5° $\Psi_{2n}(z) = (1 - z^n)\Psi_n(-z)$, *if n is odd.*
6° $\Psi_{pn}(z) = \Psi_n(z^p)$, *if $p \mid n$.*
7° $\Psi_{pn}(z) = \Psi_n(z^p)\Phi_n(z)$, *if $p \nmid n$.*

Proof. For 1° note that for this value of n, the only non-primitive n-th roots of unity are the ones having order that divides $p^\alpha - 1$. These are the roots of the polynomial $z^{p^{\alpha-1}} - 1$ and the conclusion follows.

2° follows immediately from the fact that $\varphi(n) = (p_1 - 1)\cdots(p_k - 1)$.

Let us prove 3°. The only non-primitive n-th roots of unity have orders 1, p or q. Hence, these are the roots of the polynomials $z^p - 1$ and $z^q - 1$, respectively. As the root 1 appears in both polynomials we have that

$$\Psi_n(z) = \frac{(z^p - 1)(z^q - 1)}{z - 1},$$

as required.

For 4°, note that the non-primitive pqr-th roots of unity are the roots of unity of order dividing pq, qr or rp. Denoting by U_k the set of roots of unity which have order dividing k, using the Principle of Inclusion and Exclusion, we deduce that

$$|U_{pq} \cup U_{qr} \cup U_{rp}| = |U_{pq}| + |U_{qr}| + |U_{rp}| - |U_p| - |U_q| - |U_r| + |U_1|.$$

The elements of $U_{pq} \cup U_{qr} \cup U_{rp}$ are the roots of Ψ_n. The conclusion follows by identifying the roots of unity with the roots of the corresponding polynomials.

To prove 5°, one just observe that the non-primitive $2n$-th roots of unity have order dividing n or $2d$, where $d \mid n$ and $d < n$. The first ones are the roots of $1 - z^n$, whereas the second type can be found among the roots of $\Psi_n(-z)$. The statements 5° and 6° can be proved in a similar fashion. □

From the proposition above, we easily derive the following corollary.

Corollary 8.5. *1. If p,q are distinct primes, then the cyclotomic polynomial*

$$\Phi_{pq}(z) = \frac{(z^{pq} - 1)(z - 1)}{(z^p - 1)(z^q - 1)}.$$

2. Moreover, if p,q,r are distinct primes, then the cyclotomic polynomial

$$\Phi_{pqr}(z) = \frac{(z^{pqr} - 1)(z^p - 1)(z^q - 1)(z^r - 1)}{(z^{pq} - 1)(z^{qr} - 1)(z^{rp} - 1)(z - 1)}.$$

8.7.1 The coefficients of Ψ_n

Since Ψ_n is the division of the monic polynomial $z^n - 1$ and the cyclotomic polynomial Φ_n, both have integer coefficients, it follows that Ψ_n is monic with integer coefficients as well. As mentioned in the beginning of the section, Ψ_n is intimately connected to the cyclotomic polynomial Φ_n. This suggests that understanding the coefficients of Ψ_n is a challenging venture, as any knowledge above the coefficients of Ψ_n could be transferred to knowledge about the coefficients of Φ_n and vice-versa.

Using the generalized binomial coefficient

$$\binom{\alpha}{j} = \frac{\alpha(\alpha-1)\cdots(\alpha-j+1)}{j!}, \quad \alpha \in \mathbb{R}, j \in \mathbb{N},$$

we establish the following formula, analogous to (8.16).

Theorem 8.12. *For every $m, n \in \mathbb{N}$, $n \geq 1$, the following formula holds*

$$d_m^{(n)} = \sum_{i_1+2i_2+\ldots+mi_m=m} (-1)^{i_1+\cdots+i_m+1} \binom{-\mu(n)}{i_1}\binom{-\mu(n/2)}{i_2}\cdots\binom{-\mu(n/m)}{i_m} \tag{8.37}$$

Proof. We make use of the infinite product formula established in (8.15), namely $\Phi_n(z) = \prod_{d=1}^{\infty} \left(1-z^d\right)^{\mu(n/d)}$. After observing that

$$\begin{aligned}\Psi_n(z) = \frac{z^n-1}{\Phi_n(z)} &= (z^n-1)\prod_{d=1}^{\infty}(1-z^d)^{-\mu(n/d)} \\ &= (z^n-1)\sum_{m=0}^{\infty}\left(\sum_{i_1+2i_2+\cdots+mi_m=m}(-1)^{i_1+\cdots+i_m}\binom{-\mu(n)}{i_1}\binom{-\mu(n/2)}{i_2}\right. \\ &\left.\cdots\binom{-\mu(n/m)}{i_m}\right)z^m,\end{aligned}$$

the formula follows by identifying coefficients of z^m on both sides. □

Let us emphasize how one can compute the first few coefficients of Ψ_n, for every $n \in \mathbb{N}^*$ using the formula above.

- For $m = 1$, we have $i_1 = 1$, hence $d_1^{(n)} = \binom{-\mu(n)}{1} = -\mu(n)$.
- For $m = 2$, the equation $i_1 + 2i_2 = 2$ has the solutions $(i_1, i_2) = (2,0)$ and $(i_1, i_2) = (0,1)$, so one obtains

$$d_2^{(n)} = -\binom{-\mu(n)}{2} + \binom{-\mu(n/2)}{1} = -\frac{1}{2}\mu(n)(\mu(n)+1) - \mu(n/2).$$

- For $m = 3$, the solutions to (l_1, l_2, l_3) of the equation $l_1 + 2l_2 + 3l_3 = 3$ are $(3,0,0)$, $(1,1,0)$ and $(0,0,1)$, therefore one obtains

$$\begin{aligned}d_3^{(n)} &= \binom{-\mu(n)}{3} - \binom{-\mu(n)}{1}\binom{-\mu(n/2)}{1} + \binom{-\mu(n/3)}{1} \\ &= -\frac{1}{2}\left(\mu(n)^2 + \mu(n)\right) - \mu(n)\mu(n/2) - \mu(n/3),\end{aligned}$$

where we have used again that $\mu^3 = \mu$.

- For $m=4$, the solutions (l_1,l_2,l_3,l_4) of the equation $l_1+2l_2+3l_3+4l_4=4$ are $(4,0,0,0)$, $(2,1,0,0)$, $(0,2,0,0)$, $(1,0,1,0)$, $(0,0,0,1)$, hence

$$\begin{aligned} d_4^{(n)} &= -\binom{-\mu(n)}{4}+\binom{-\mu(n)}{2}\binom{-\mu(n/2)}{1}-\binom{-\mu(n)}{1}\binom{-\mu(n/3)}{1}+\\ &+\binom{-\mu(n/2)}{2}+\binom{-\mu(n/4)}{1}\\ &=-\frac{\mu(n)(\mu(n)+1)}{2}-\frac{\mu(n)(\mu(n)+1)}{2}\mu(n/2)-\mu(n)\mu(n/3)+\\ &+\frac{\mu(n/2)(\mu(n/2)+1)}{2}-\mu(n/4), \end{aligned}$$

  where we have used the identity (8.21) to simplify the computations and deduce that $\binom{-\mu(n)}{4}=\binom{-\mu(n)}{2}$.

Remark. If one knows the first few coefficients $d_k^{(n)}$, one can directly compute the coefficients $c_k^{(n)}$ of the cyclotomic polynomial, for small values of k. This can be achieved by identifying the coefficients in $\Phi_n(z)\cdot\Psi_n(z)=z^n-1$. This reduced to solving the linear system

$$\begin{cases} c_0^{(n)}d_0^{(n)}=-1\\ c_0^{(n)}d_1^{(n)}+c_1^{(n)}d_0^{(n)}=0\\ c_0^{(n)}d_2^{(n)}+c_1^{(n)}d_1^{(n)}+c_2^{((n)}d_0^{(n)}=0\\ \qquad\qquad\vdots \end{cases},$$

where the coefficients $c_0^{(n)}$, $c_1^{(n)}$, $c_2^{(n)}$, … of Φ_n are the unknowns.

We use Newton's identities for Ψ_n to find a recurrence relation for the coefficients $d_k^{(n)}$. Denote P_j the j-th symmetric power polynomial evaluated at the $\varphi(n)$ roots of Φ_n (primitive roots of unity) and P_j', for the j-th symmetric power polynomial evaluated at the $n-\varphi(n)$ roots of Ψ_n. Recall that in Example 8.12 we had $\delta_j(n)=\sum_{a=1}^{n}\left(e^{2\pi i\frac{a}{n}}\right)^j$, where $\delta_j(n)=\begin{cases} n \text{ if } n\mid j\\ 0 \text{ if } n\nmid j\end{cases}$.

In our notation, the symmetric power sums polynomials satisfy the relation $P_j+Pj'=\delta_j(n)$. But for $j<n$ we have $n\nmid j$, hence $P_j'=-P_j=-\rho(n,j)$, where ρ denotes the Ramanujan sum (8.6). The polynomial Ψ_n is antireciprocal, hence we have the relations

$$S_j'=(-1)^j d_{n-\varphi(n)-j}^{(n)}=(-1)^{j+1}d_j^{(n)},\ j=1,2,\ldots,$$

where S_j' is the evaluation of the j-th fundamental symmetric polynomial at the $n-\varphi(n)$ roots of Ψ_n. The explanation above implies that the following recurrence holds.

Theorem 8.13. *The coefficients of Ψ_n satisfy the following recurrence relation involving Ramanujan sums:*

$$d_k^{(n)} = \frac{1}{k}\left[-\rho(n,k) + \rho(n,k-1)d_1^{(n)} + \cdots + \rho(n,1)d_{k-1}^{(n)}\right] \tag{8.38}$$

Let us apply the theorem above to give a different way for computing the first four coefficients $d_k^{(n)}$, for every $n \in \mathbb{N}^*$, recovering the results obtained right after Theorem 8.12.

- For $k = 1$, we have $d_1^{(n)} = -\rho(n,1) = -\mu(n)$.
- For $k = 2$, one obtains

$$\begin{aligned} d_2^{(n)} &= \frac{1}{2}\left[-\rho(n,2) + \rho(n,1)d_1^{(n)}\right] = -\frac{1}{2}\left[\mu(n) + 2\mu(n/2) + \mu^2(n)\right] \\ &= -\frac{\mu^2(n) + \mu(n)}{2} - \mu(n/2). \end{aligned}$$

- For $k = 3$, using the identity $\mu^3 = \mu$, it follows that

$$\begin{aligned} d_3^{(n)} &= \frac{1}{3}\left[-\rho(n,3) + \rho(n,2)d_1^{(n)} + \rho(n,1)d_2^{(n)}\right] \\ &= \frac{1}{3}\left[-\mu(n) - 3\mu(n/3) - (\mu(n) + 2\mu(n/2))\,\mu(n) + \right. \\ &\quad \left. + \mu(n)\left(-\frac{\mu(n)^2 + \mu(n)}{2} - \mu(n/2)\right)\right] \\ &= -\frac{1}{2}\left(\mu(n)^2 + \mu(n)\right) - \mu(n)\mu(n/2) - \mu(n/3) \end{aligned}$$

- For $k = 4$, using again the identity $\mu^3 = \mu$ we get

$$\begin{aligned} d_4^{(n)} &= \frac{1}{4}\left[-\rho(n,4) + \rho(n,3)d_1^{(n)} + \rho(n,2)d_2^{(n)} + \rho(n,1)d_3^{(n)}\right] \\ &= \frac{1}{4}\left[-\mu(n) - 2\mu(n/2) - 4\mu(n/4) - (\mu(n) + 3\mu(n/3))\,\mu(n) + \right. \\ &\quad + (\mu(n) + 2\mu(n/2))\left(\frac{\mu(n)^2 - \mu(n)}{2} - \mu(n/2)\right) + \\ &\quad \left. + \mu(n)\left(-\frac{1}{2}\left(\mu(n)^2 + \mu(n)\right) - \mu(n)\mu(n/2) - \mu(n/3)\right)\right] \\ &= -\frac{\mu(n)(\mu(n)+1)}{2} - \frac{\mu(n)(\mu(n)+1)}{2}\mu(n/2) - \mu(n)\mu(n/3) + \\ &\quad + \frac{\mu(n/2)(\mu(n/2)+1)}{2} - \mu(n/4). \end{aligned}$$

As in the case of cyclotomic polynomials, the recurrence relation 8.38 suggests that every coefficient $d_k^{(n)}$ of Ψ_n is a polynomial with rational coefficients in the variables given by the Ramanujan sums $\rho(n,k)$, where $k = 1,2,\ldots,n-\varphi(n)-1$. This is illustrated in the following result, a direct consequence of Theorem 7.3.

Theorem 8.14. *We have*

$$d_k^{(n)} = -\sum_{l_1+2l_2+\cdots+kl_k=k} \frac{\rho(n,1)^{l_1}}{1^{l_1}l_1!}\cdot\frac{\rho(n,2)^{l_2}}{2^{l_2}l_2!}\cdots\frac{\rho(n,k)^{l_k}}{k^{l_k}l_k!}. \tag{8.39}$$

In the proof, we have use the relations $P_j' = -\rho(n,j)$ and $S_k' = (-1)^{k+1}d_k^{(n)}$.

Let us compute the first four coefficients of Ψ_n, for every $n \in \mathbb{N}^*$, using the formula (8.39).

- For $k = 1$, we have $l_1 = 1$, hence $d_1^{(n)} = -\rho(n,1) = -\mu(n)$.
- For $k = 2$, the equation $i_1 + 2i_2 = 2$ has the solutions $(i_1,i_2) = (2,0)$ and $(i_1,i_2) = (0,1)$, so one obtains

$$\begin{aligned} d_2^{(n)} &= -\frac{1}{2}\rho(n,1)^2 - \frac{1}{2}\rho(n,2) \\ &= -\frac{1}{2}\mu^2(n) - \frac{1}{2}(\mu(n)+2\mu(n/2)) \\ &= -\frac{1}{2}\mu(n)(\mu(n)+1) - \mu(n/2). \end{aligned}$$

- For $k = 3$, the solutions to (l_1,l_2,l_3) of the equation $l_1 + 2l_2 + 3l_3 = 3$ are $(3,0,0)$, $(1,1,0)$ and $(0,0,1)$, therefore one obtains

$$\begin{aligned} d_3^{(n)} &= -\frac{1}{6}\rho(n,1)^3 - \frac{1}{2}\rho(n,1)\rho(n,2) - \frac{1}{3}\rho(n,3) \\ &= -\frac{1}{6}\mu^3(n) - \frac{1}{2}\mu(n)\,(\mu(n)+2\mu(n/2)) - \frac{1}{3}\,(\mu(n)+3\mu(n/3)) \\ &= -\frac{1}{2}(\mu^2(n)+\mu(n)) - \mu(n)\mu(n/2) - \mu(n/3), \end{aligned}$$

  where we used the relation $\mu^3 = \mu$.
- For $k = 4$, the solutions (l_1,l_2,l_3,l_4) of the equation $l_1 + 2l_2 + 3l_3 + 4l_4 = 4$ are $(4,0,0,0)$, $(2,1,0,0)$, $(0,2,0,0)$, $(1,0,1,0)$, $(0,0,0,1)$, hence

$$\begin{aligned}
d_4^{(n)} &= -\frac{1}{24}\rho(n,1)^4 - \frac{1}{4}\rho(n,1)^2\rho(n,2) - \frac{1}{3}\rho(n,1)\rho(n,3) \\
&\quad - \frac{1}{8}\rho(n,2)^2 - \frac{1}{4}\rho(n,4) \\
&= -\frac{1}{24}\mu^4(n) - \frac{1}{4}\mu^2(n)(\mu(n)+2\mu(n/2))^2 - \\
&\quad - \frac{1}{4}(\mu(n)+2\mu(n/2)+4\mu(n/4)) \\
&= -\frac{\mu(n)(\mu(n)+1)}{2} - \frac{\mu(n)(\mu(n)+1)}{2}\mu(n/2) - \mu(n)\mu(n/3) + \\
&\quad + \frac{\mu(n/2)(\mu(n/2)+1)}{2} - \mu(n/4).
\end{aligned}$$

In the relation above we used repeatedly the fact that $\mu^3 = \mu$.

We point out the following direct corollary.

Corollary 8.6. *For every $n \in \mathbb{N}^*$ and every $k \in \{1,2,\ldots,n-\varphi(n)\}$, the anti-cyclotomic coefficient $d_k^{(n)}$ is a polynomial with rational coefficients in $\mu(n/d)$, where d is a divisor of n. Moreover, the degree of $\mu(n/d)$ in every monomial can be at most 2.*

8.7.2 The integral formula for the coefficients of Ψ_n

Following the same process as the one used for cyclotomic polynomials, similar integral formulae can be obtained for the coefficients of $\Psi_n(z)$.

In this section we compute an integral formula for the coefficients of the inverse cyclotomic polynomial $\Psi_n(z)$ is defined by

$$\Psi_n(z) = \prod_{\substack{1\le k\le n \\ \gcd(k,n)>1}} \left(z - e^{\frac{2k\pi i}{n}}\right) = \frac{x^n-1}{\Phi_n(z)} = \sum_{j=0}^{n-\varphi(n)} d_j^{(n)} z^j. \tag{8.40}$$

The roots of this monic polynomial are the non-primitive nth roots of unity, having degree $n-\varphi(n)$ and integer coefficients $d_j^{(n)}$, $j = 0,1,\ldots,n-\varphi(n)$.

The proof of the main result uses the following known identity involving Euler's totient function.

Lemma 8.4. *Let $n \ge 3$ be a positive integer. The following formula holds:*

$$\sum_{\substack{1\le k\le n \\ \gcd(k,n)>1}} k = \frac{n}{2}\left(n+1-\varphi(n)\right). \tag{8.41}$$

Proof. Using Lemma 8.3, one can write

$$\sum_{\substack{1\le k\le n\\ \gcd(k,n)>1}} k = \sum_{k=1}^{n} k - \sum_{\substack{1\le k\le n\\ \gcd(k,n)=1}} k$$
$$= \frac{n(n+1)}{2} - \frac{n}{2}\varphi(n) = \frac{n}{2}\left(n - \varphi(n) + 1\right).$$

For n is prime one has $\varphi(n) = n-1$, hence the value of the sum is n. □

In order to get a unitary formula for $d_j^{(n)}$, we introduce the function

$$\Gamma_n(t) = \prod_{\substack{1\le k\le n\\ \gcd(k,n)>1}} \sin\left(t - \frac{k\pi}{n}\right). \tag{8.42}$$

Clearly, for $n = 1$ or when $n \ge 2$ is prime one obtains

$$\Gamma_n(t) = \sin\left(t - \frac{n\pi}{n}\right) = -\sin t.$$

For the first composite values $n = 4, 6, 8$ we have

$$\begin{aligned}
\Gamma_4(t) &= \sin\left(t - \frac{2\pi}{4}\right)\sin\left(t - \frac{4\pi}{4}\right)\\
&= \sin\left(t - \frac{\pi}{2}\right)\sin(t-\pi) = (-\cos t)(-\sin t) = \sin t\cdot\cos t\\
&= \frac{1}{2}\sin 2t.\\
\Gamma_6(t) &= \sin\left(t - \frac{2\pi}{6}\right)\sin\left(t - \frac{3\pi}{6}\right)\sin\left(t - \frac{4\pi}{6}\right)\sin\left(t - \frac{6\pi}{6}\right)\\
&= \sin\left(t - \frac{\pi}{3}\right)\sin\left(t - \frac{\pi}{2}\right)\sin\left(t - \frac{2\pi}{3}\right)\sin(t-\pi)\\
&= \frac{1}{8}\left(\sin 2t + \sin 4t\right).\\
\Gamma_8(t) &= \sin\left(t - \frac{2\pi}{8}\right)\sin\left(t - \frac{4\pi}{8}\right)\sin\left(t - \frac{6\pi}{8}\right)\sin\left(t - \frac{8\pi}{8}\right)\\
&= \frac{1}{8}\sin 4t.
\end{aligned}$$

In what follows we assume $n \ge 3$.

Theorem 8.15. *The coefficients $d_j^{(n)}$, $j = 0, 1, \ldots, n - \varphi(n)$, of the inverse cyclotomic polynomial $\Psi_n(z)$ are given by the following integral formula:*

$$d_j^{(n)} = (-1)^{n+1}\frac{2^{n-\varphi(n)}}{\pi}\int_0^{\pi}\Gamma_n(t)\cdot\sin\left(n-\varphi(n)-2j\right)t\,\mathrm{d}t. \tag{8.43}$$

Proof. Denoting $\zeta_n = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$ and $z = \cos 2t + i\sin 2t$ for $t\in[0,2\pi]$, $k = 1,\ldots,n$, the previous calculations showed that

$$z-\zeta_n^k = 2i\sin\left(t-\frac{k\pi}{n}\right)\left[\cos\left(t+\frac{k\pi}{n}\right)+i\sin\left(t+\frac{k\pi}{n}\right)\right].$$

To simplify the notation we shall use $\cos t + i\sin t$ by $\exp(ti)$.

By Lemma 8.4, for $n\geq 3$, one can write the polynomial $\Psi_n(z)$ in the form

$$\begin{aligned}
\Psi_n(z) &= \prod_{\substack{1\leq k\leq n\\ \gcd(k,n)>1}}(z-\zeta_n^k)\\
&= (2i)^{n-\varphi(n)}\prod_{\substack{1\leq k\leq n\\ \gcd(k,n)>1}}\sin\left(t-\frac{k\pi}{n}\right)\exp\left(ti+\frac{k\pi}{n}i\right)\\
&= (2i)^{n-\varphi(n)}\Gamma_n(t)\exp\left(\left[n-\varphi(n)\right]ti+\left[n-\varphi(n)+1\right]\frac{\pi}{2}i\right)\\
&= (2i)^{n-\varphi(n)}\Gamma_n(t)\left[\cos\left(n-\varphi(n)t\right)+i\sin\left(n-\varphi(n)t\right)\right]\cdot i^{n-\varphi(n)+1}\\
&= 2^{n-\varphi(n)}(-1)^{n-\varphi(n)}\Gamma_n(t)\left[\cos\left(n-\varphi(n)t\right)+i\sin\left(n-\varphi(n)t\right)\right]i\\
&= (-2)^{n-\varphi(n)}\Gamma_n(t)\left[\cos\left(n-\varphi(n)t\right)+i\sin\left(n-\varphi(n)t\right)\right]i,
\end{aligned}$$

where we have used that $\varphi(n)$ is even for $n\geq 3$, and that $e^{\frac{\pi}{2}i} = i$.

For every $j = 0,1,\ldots,\varphi(n)$, one may write

$$\begin{aligned}
&d_j^{(n)} + \sum_{k\neq j} d_k^{(n)} z^{k-j} = z^{-j}\prod_{\substack{1\leq k\leq n\\ \gcd(k,n)>1}}(z-\zeta_n^k)\\
&= (-2)^{n-\varphi(n)}\Gamma_n(t)\left(\cos 2jt - i\sin 2jt\right)\left[\cos\left(n-\varphi(n)t\right)+i\sin\left(n-\varphi(n)t\right)\right]i\\
&= (-2)^{n-\varphi(n)}\Gamma_n(t)\left[\cos\left(n-\varphi(n)-2j\right)t+i\sin\left(n-\varphi(n)-2j\right)t\right]i\\
&= (-1)^{n+1}2^{n-\varphi(n)}\Gamma_n(t)\left[\sin\left(n-\varphi(n)-2j\right)t-i\cos\left(n-\varphi(n)-2j\right)t\right].
\end{aligned}$$

Integrating on the interval $[0,2\pi]$ we obtain formula (8.43). This is true since the integral of z^{k-j} over $[0,2\pi]$ vanishes whenever $k\neq j$. □

Furthermore, by the proof of formula (8.43) we deduce that

$$\int_0^{\pi}\Gamma_n(t)\cos(n-\varphi(n)-2j)t\,\mathrm{d}t = 0,\quad j = 0,1,\ldots,n-\varphi(n). \tag{8.44}$$

8.7.3 Some applications of the integral formula

Using formula (8.43) we show that the inverse cyclotomic polynomial is antipalindromic, and we derive compact integral formulae for the mid-term of cyclotomic polynomials, the direct, and alternate sums of coefficients.

Reciprocal coefficients. These add to zero. Here we give an elegant proof based on the integral formula (8.43).

Theorem 8.16. *The inverse cyclotomic polynomial $\Psi_n(z)$ is antipalindromic, that is its coefficients satisfy the following antisymmetry relation*

$$d_j^{(n)} = -d_{n-\varphi(n)-j}^{(n)}, \quad j = 0,1,\ldots,n-\varphi(n). \tag{8.45}$$

Proof. Using formula (8.43), for every $j = 0,1,\ldots,\varphi(n)$, we have

$$\begin{aligned} d_{n-\varphi(n)-j}^{(n)} &= (-1)^{n+1}\frac{2^{n-\varphi(n)}}{\pi}\int_0^\pi \Gamma_n(t)\sin\left(n-\varphi(n)-2(n-\varphi(n)-j)\right)t\,\mathrm{d}t \\ &= (-1)^{n+1}\frac{2^{n-\varphi(n)}}{\pi}\int_0^\pi \Gamma_n(t)\sin\left(2j+\varphi(n)-n\right)t\,\mathrm{d}t \\ &= -(-1)^{n+1}\frac{2^{n-\varphi(n)}}{\pi}\int_0^\pi \Gamma_n(t)\sin\left(n-\varphi(n)-2j\right)t\,\mathrm{d}t \\ &= -d_j^{(n)}. \end{aligned}$$

This ends the proof. □

The mid-term coefficients of $\Psi_n(z)$. Recall that $\varphi(n)$ is even for $n \geq 3$. Hence, if n is odd then $n-\varphi(n)$ is odd, and there is no middle coefficient. If n is even, then the middle term coefficient index is given by the formula

$$j = \frac{n-\varphi(n)}{2}.$$

Since $n-\varphi(n)-2j = 0$, from formula (8.43) we obtain

$$d_{\frac{n-\varphi(n)}{2}}^{(n)} = (-1)^{n+1}\frac{2^{n-\varphi(n)}}{\pi}\int_0^\pi \Gamma_n(t)\sin(0t)\,\mathrm{d}t = 0. \tag{8.46}$$

Direct sum of coefficients $\Psi_n(1)$. From the definition of $\Psi_n(z)$, one obtains

$$\Psi_n(1) = \sum_{j=0}^{n-\varphi(n)} d_j^{(n)} = 0.$$

This can also be checked by formula (8.45), which gives

$$\Psi_n(1) = \sum_{j=0}^{n-\varphi(n)} d_j^{(n)} = \sum_{j=0}^{\left\lfloor \frac{n-\varphi(n)}{2} \right\rfloor} \left(d_j^{(n)} + d_{n-\varphi(n)-j}^{(n)} \right).$$

Indeed, when n is odd this sum covers all the terms, while when n is even the middle term obtained for $j = \frac{n-\varphi(n)}{2}$ is zero.

This is in contrast with the more complicated formula (8.32) for $\Phi_n(1)$.

Alternate sum of coefficients $\Psi_n(-1)$. By the formula (8.35) for $\Phi_n(z)$ and the definition of $\Psi_n(z)$ one can write

$$\Psi_n(-1) = \frac{(-1)^n - 1}{\phi_n(-1)} = \begin{cases} 0 & \text{if } n \text{ is even} \\ 2 & \text{if } n \text{ is odd,} \end{cases} \tag{8.47}$$

where p is prime.

From the formula (8.30) for the coefficients $d_j^{(n)}$, we obtain an integral equivalent formula $\Psi_n(-1)$, valid for $n \geq 3$, as follows

$$\begin{aligned} \Psi_n(-1) &= \sum_{j=0}^{n-\varphi(n)} d_j^{(n)} (-1)^j \\ &= (-1)^{n+1} \sum_{j=0}^{n-\varphi(n)} \frac{2^{n-\varphi(n)}}{\pi} \int_0^\pi \Gamma_n(t) (-1)^j \sin(n-\varphi(n)-2j)t \, \mathrm{d}t, \\ &= (-1)^{n+1} \frac{2^{n-\varphi(n)}}{\pi} \int_0^\pi \Gamma_n(t) \left[\sum_{j=0}^{n-\varphi(n)} (-1)^j \sin(n-\varphi(n)-2j)t \right] \mathrm{d}t \\ &= \left(1 + (-1)^{n+1}\right) \frac{2^{n-\varphi(n)-1}}{\pi} \int_0^\pi \Gamma_n(t) \frac{\sin(n-\varphi(n)+1)t}{\cos t} \, \mathrm{d}t. \end{aligned} \tag{8.48}$$

To prove the last identity note that for a fixed $j \in \{0, \ldots, n-\varphi(n)\}$, one has

$$\begin{aligned} (-1)^j \sin(n-\varphi(n)-2j)t &= \sin\left[(n-\varphi(n)-2j)t - j\pi\right] \\ &= \sin\left[(n-\varphi(n))\,t - 2j\left(t + \frac{\pi}{2}\right)\right]. \end{aligned}$$

Multiplying this expression by $2\sin\left(t + \frac{\pi}{2}\right)$ one obtains

$$\begin{aligned} &2(-1)^j \sin(n-\varphi(n)-2j)t \cdot \sin\left(t + \frac{\pi}{2}\right) \\ &= \cos\left[(n-\varphi(n))\,t - (2j+1)\left(t + \frac{\pi}{2}\right)\right] \\ &- \cos\left[(n-\varphi(n))\,t - (2j-1)\left(t + \frac{\pi}{2}\right)\right]. \end{aligned}$$

Summing for $j \in \{0,\dots,n-\varphi(n)\}$ we obtain the telescopic sum

$$\begin{aligned}
&\sum_{j=0}^{n-\varphi(n)} (-1)^j \cdot \sin(n-\varphi(n)-2j)t \cdot \sin\left(t+\frac{\pi}{2}\right) \\
&= -\frac{1}{2}\left[\cos\left((n-\varphi(n)+1)t+\frac{\pi}{2}\right)\right] \\
&+ \frac{1}{2}\left[\cos\left(-(n-\varphi(n)+1)t-\frac{\pi}{2}-(n-\varphi(n))\,\pi\right)\right] \\
&= \frac{1}{2}\left[\sin\left((n-\varphi(n)+1)t\right)-(-1)^{n-\varphi(n)}\sin\left((n-\varphi(n)+1)t\right)\right], \\
&= \frac{1+(-1)^{n-\varphi(n)+1}}{2}\cdot\frac{\sin(n-\varphi(n)+1)t}{\cos t}.
\end{aligned}$$

where we used $\cos(x+k\pi) = (-1)^k \cos x$, $k \in \mathbb{Z}$, $\cos(x+\pi/2) = -\sin x$, $\cos(x-\pi/2) = \sin x$. The results follows, as $\varphi(n)$ is even for $n \geq 3$.

If $n \geq 3$ is odd, the function $f : [0,\pi] \setminus \{\pi/2\} \mapsto \mathbb{R}$ defined by the formula

$$f(t) = \frac{\sin(n-\varphi(n)+1)t}{\cos t}$$

can be extended by continuity at $\pi/2$ as

$$\lim_{t\to\pi/2} f(t) = (-1)^{\frac{n-\varphi(n)-1}{2}}\,(n-\varphi(n)+1)\,.$$

Hence, we obtain the following result.

Corollary 8.7. *If $n \geq 3$ is odd, then*

$$\int_0^{\pi} \Gamma_n(t)\frac{\sin(n-\varphi(n)+1)t}{\cos t}\,\mathrm{d}t = \frac{\pi}{2^{n-\varphi(n)-1}}.$$

8.8 Upper bounds for the coefficients

In this section we use the integral formulae for the coefficients of Φ_n and Ψ_n to establish upper bounds, which we illustrate via numerical simulations. These involve some special integrals which we aim to explore in future papers. The section is largely based on the recent results published in [29].

8.8.1 Upper bounds for the coefficients of Φ_n

The integral formula (8.30) can be used to establish upper bounds for the coefficients of the cyclotomic polynomial Φ_n.

Theorem 8.17. *For $n \geq 3$, the following property holds*

$$\left|c_j^{(n)}\right| \leq \frac{2^{\varphi(n)}}{\sqrt{2\pi}} \sqrt{\int_0^\pi \Lambda_n^2(t)\,\mathrm{d}t}, \quad j = 0,1,\ldots,\varphi(n). \tag{8.49}$$

Proof. Indeed, by the Cauchy-Schwarz integral inequality we have

$$\begin{aligned}
\left|c_j^{(n)}\right|^2 &= \frac{2^{2\varphi(n)}}{\pi^2} \left(\int_0^\pi \Lambda_n(t) \cdot \cos\left(\varphi(n) - 2j\right) t\,\mathrm{d}t\right)^2 \\
&\leq \frac{2^{2\varphi(n)}}{\pi^2} \int_0^\pi \Lambda_n^2(t)\,\mathrm{d}t \cdot \int_0^\pi \cos^2\left(\varphi(n) - 2j\right) t\,\mathrm{d}t \\
&= \frac{2^{2\varphi(n)}}{\pi^2} \int_0^\pi \Lambda_n^2(t)\,\mathrm{d}t \cdot \int_0^\pi \frac{1 + \cos 2\left(\varphi(n) - 2j\right) t}{2}\,\mathrm{d}t \\
&= \frac{2^{2\varphi(n)}}{\pi^2} \int_0^\pi \Lambda_n^2(t)\,\mathrm{d}t \left(\frac{\pi}{2} + \frac{\sin 2\left(\varphi(n) - 2j\right) t}{4\left(\varphi(n) - 2j\right)}\Bigg|_{t=0}^{t=\pi}\right) \\
&= \frac{2^{2\varphi(n)}}{2\pi} \int_0^\pi \Lambda_n^2(t)\,\mathrm{d}t.
\end{aligned}$$

Taking the square root we obtain the desired result. In the calculations we used $\cos^2 x = \frac{1+\cos 2x}{2}$ to show that $\int_0^\pi \cos^2\left(\varphi(n) - 2j\right) t\,\mathrm{d}t = \frac{\pi}{2}$. □

Notice that the integral $\int_0^\pi \Lambda_n^2(t)\,\mathrm{d}t$ played an important role in establishing the upper bound (8.49) for the coefficients of Φ_n and will be examined numerically. Next we provide a lower bound. Since $c_0^{(n)} = 1$ one obtains

$$c_0^{(n)} = \frac{2^{\varphi(n)}}{\pi} \int_0^\pi \Lambda_n(t) \cos\varphi(n) t\,\mathrm{d}t = 1, \tag{8.50}$$

from where we obtain

$$\begin{aligned}
\frac{\pi^2}{2^{2\varphi(n)}} &= \left(\int_0^\pi \Lambda_n(t) \cos\varphi(n) t\,\mathrm{d}t\right)^2 \\
&\leq \int_0^\pi \Lambda_n^2(t)\,\mathrm{d}t \cdot \int_0^\pi \cos^2\varphi(n) t\,\mathrm{d}t = \frac{\pi}{2} \cdot \int_0^\pi \Lambda_n^2(t)\,\mathrm{d}t,
\end{aligned}$$

which gives the lower bound

$$\frac{2\pi}{2^{2\varphi(n)}} \leq \int_0^\pi \Lambda_n^2(t)\,\mathrm{d}t. \tag{8.51}$$

8.8.2 Upper bounds for the coefficients of Ψ_n

An upper bound for the coefficients of the inverse cyclotomic polynomial Ψ_n can be obtained as follows.

Theorem 8.18. *For $n \geq 3$, the following inequality holds:*

$$\left|d_j^{(n)}\right| \leq \frac{2^{n-\varphi(n)}}{\sqrt{2\pi}} \sqrt{\int_0^\pi \Gamma_n^2(t)\,\mathrm{d}t}, \quad j = 0,1,\ldots,n-\varphi(n). \tag{8.52}$$

Proof. By the Cauchy-Schwarz integral inequality we have

$$\begin{aligned}
\left|d_j^{(n)}\right|^2 &= \frac{2^{2(n-\varphi(n))}}{\pi^2} \left(\int_0^\pi \Gamma_n(t) \cdot \sin\left(n-\varphi(n)-2j\right)t\,\mathrm{d}t\right)^2 \\
&\leq \frac{2^{2(n-\varphi(n))}}{\pi^2} \int_0^\pi \Gamma_n^2(t)\,\mathrm{d}t \cdot \int_0^\pi \sin^2\left(n-\varphi(n)-2j\right)t\,\mathrm{d}t \\
&= \frac{2^{2(n-\varphi(n))}}{\pi^2} \int_0^\pi \Gamma_n^2(t)\,\mathrm{d}t \cdot \int_0^\pi \frac{1-\cos 2\left(n-\varphi(n)-2j\right)t}{2}\,\mathrm{d}t \\
&= \frac{2^{2(n-\varphi(n))}}{\pi^2} \int_0^\pi \Gamma_n^2(t)\,\mathrm{d}t \left(\frac{\pi}{2} - \frac{\sin 2\left(n-\varphi(n)-2j\right)t}{4\left(n-\varphi(n)-2j\right)}\Bigg|_{t=0}^{t=\pi}\right) \\
&= \frac{2^{2(n-\varphi(n))}}{2\pi} \int_0^\pi \Gamma_n^2(t)\,\mathrm{d}t.
\end{aligned}$$

Taking the square root we obtain the desired result. In the calculations we used $\sin^2 x = \frac{1-\cos 2x}{2}$ to show that $\int_0^\pi \sin^2\left(n-\varphi(n)-2j\right)t\,\mathrm{d}t = \frac{\pi}{2}$. □

Furthermore, since $d_0^{(n)} = -1$, one obtains the lower bound

$$\frac{2\pi}{2^{2(n-\varphi(n))}} \leq \int_0^\pi \Gamma_n^2(t)\,\mathrm{d}t. \tag{8.53}$$

We notice that the integral $\int_0^\pi \Gamma_n^2(t)\,\mathrm{d}t$ played an important role in establishing the upper bound for the coefficients (8.52).

8.8.3 Numerical simulations

In this section, we explore the upper bounds of the cyclotomic and inverse cyclotomic polynomial coefficients and investigate some related integrals. As seen earlier, the functions $\Lambda_n(t)$ and $\Gamma_n(t)$ played an important role in the exact integral formulae for the coefficients $c_j^{(n)}$ of Φ_n and $d_j^{(n)}$ of Ψ_n, while and $\Lambda_n^2(t)$ and $\Gamma_n^2(t)$ featured in formulae for their upper bounds. The first few sequence terms ($n = 1,\ldots,20$) are displayed in Table 8.1.

The diagrams are obtained in Matlab®, and the integrals are computed by the trapezium rule with 10000 equally spaced points in the interval $[0,\pi]$.

Upper bounds for polynomial coefficients. The upper bound formula (8.49) for the coefficients $c_j^{(n)}$ of Φ_n, gives the sequence

$$ub(c_j^{(n)}) = \frac{2^{\varphi(n)}}{\sqrt{2\pi}} \sqrt{\int_0^\pi \Lambda_n^2(t)\,\mathrm{d}t}.$$

Similarly, the upper bound (8.52) of the coefficients $d_j^{(n)}$ of Ψ_n defines

$$ub(d_j^{(n)}) = \frac{2^{n-\varphi(n)}}{\sqrt{2\pi}} \sqrt{\int_0^\pi \Gamma_n^2(t)\,\mathrm{d}t}.$$

These two sequences are plotted in Figure 8.1 (c).

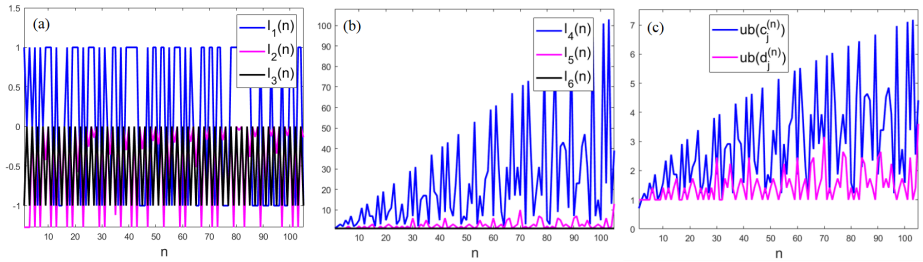

Fig. 8.1 Terms $n = 1,\ldots,105$ terms of the sequences (a) $I_1(n)$, $I_2(n)$, $I_3(n)$; (b) $I_4(n)$, $I_5(n)$, $I_6(n)$; (c) $ub(c_j^{(n)})$ and $ub(d_j^{(n)})$.

The normalised integral of Λ_n. The function $\Lambda_n(t)$ defined in (8.29) appears in the formula (8.30) for the coefficients $c_j^{(n)}$, $j = 0,1,\ldots,\varphi(n)$, of the polynomial Φ_n. The normalised integral produces the sequence of middle term coefficients of Φ_n, seen in (8.34):

$$I_1(n) = \frac{2^{\varphi(n)}}{\pi} \int_0^\pi \Lambda_n(t)\mathrm{d}t = c^{(n)}_{\frac{\varphi(n)}{2}}, \tag{8.54}$$

with the numerical values for $n \geq 2$ given by

$$0,1,0,1,-1,1,0,1,1,\ldots,$$

indexed as A094754 in OEIS.

n	$I_1(n)$	$I_2(n)$	$I_3(n)$	$I_4(n)$	$I_5(n)$	$I_6(n)$	$ub(c_j^{(n)})$	$ub(d_j^{(n)})$
1	1	-1.273	-1	1	1	1	0.707	1
2	0	-1.273	0	2	1	1	1	1
3	1	-1.273	-1	3	1	1	1.224	1
4	0	0	0	2	1	1	1	1
5	1	-1.273	-1	5	1	1	1.581	1
6	-1	0	0	3	2	1	1.224	1.414
7	1	-1.273	-1	7	1	1	1.870	1
8	0	0	0	2	1	1	1	1
9	1	-0.424	-1	3	1	1	1.224	1
10	1	0	0	5	2	1	1.581	1.4142
11	1	-1.273	-1	11	1	1	2.345	1
12	-1	0	0	3	2	1	1.224	1.414
13	1	-1.273	-1	13	1	1	2.549	1
14	-1	0	0	7	2	1	1.870	1.4142
15	-1	-0.861	-1	7	3	1	1.870	1.732
16	0	0	0	2	1	1	1	1
17	1	-1.273	-1	17	1	1	2.915	1
18	-1	0	0	3	2	1	1.224	1.414
19	1	-1.273	-1	19	1	1	3.082	1
20	1	0	0	5	2	1	1.581	1.414

Table 8.1 Values of the sequences $I_1(n)$, $I_2(n)$, $I_3(n)$, $I_4(n)$, $I_5(n)$, $I_6(n)$, $ub(c_j^{(n)})$ and $ub(d_j^{(n)})$, computed for $n = 1,\ldots,20$.

The normalised integral of Γ_n. The function $\Gamma_n(t)$ defined in (8.42) appears in formula (8.43) for the coefficients $d_j^{(n)}$, $j = 0,1,\ldots,n-\varphi(n)$, of the polynomial Ψ_n. The normalised integral

$$I_2(n) = \frac{2^{n-\varphi(n)}}{\pi} \int_0^\pi \Gamma_n(t)\mathrm{d}t, \tag{8.55}$$

links to formula (8.46) (although the middle coefficient of Ψ_n vanishes).

The normalised integral of $P_n = \Lambda_n \cdot \Gamma_n$. Consider the function

$$P_n(t) = \Lambda_n(t) \cdot \Gamma_n(t) = \prod_{1\le k\le n} \sin\left(t - \frac{k\pi}{n}\right). \tag{8.56}$$

It can be shown that

$$\int_0^\pi P_n(t)\,\mathrm{d}t = \begin{cases} 0 & \text{if } n \text{ is even} \\ -\frac{1}{n\cdot 2^{n-2}} & \text{if } n \text{ is odd.} \end{cases} \tag{8.57}$$

In Figure 8.1 (a) we plot the normalized integral

$$I_3(n) = n2^{n-2} \cdot \int_0^\pi P_n(t)\,\mathrm{d}t. \tag{8.58}$$

The normalised integral of Λ_n^2. This integral featured in the upper bound of the coefficients $c_j^{(n)}$ in (8.49). In Figure 8.1 we plot the normalized integral

$$I_4(n) = \frac{2^{2\varphi(n)}}{\pi} \int_0^\pi \Lambda_n^2(t) \mathrm{d}t. \tag{8.59}$$

The first few terms of this sequence are

$$2,3,2,5,3,7,2,3,5,11,3,13,7,7,2,17,3,\ldots,$$

which seem to correspond to A051664 in the OEIS, counting the number of nonzero coefficients in the n-th cyclotomic polynomial Φ_n.

The normalised integral of Γ_n^2. The integral of Γ_n^2 featured in the upper bound of the coefficients $d_j^{(n)}$ in (8.52). From (8.53) we have that $I_5(n) \geq 1$. In Figure 8.1 we plot the normalized integral

$$I_5(n) = \frac{2^{2(n-\varphi(n))}}{2\pi} \int_0^\pi \Gamma_n^2(t) \mathrm{d}t. \tag{8.60}$$

The first few terms are

$$1,1,1,1,2,1,1,1,2,1,2,\ldots,$$

seeming to indicate the sequence A001221 in OEIS, number of distinct primes dividing n, whose terms are half of those in sequence A034444 (representing the number of unitary divisors of n (divisors d of n, for which $\gcd(d, n/d) = 1$).

The normalised integral of P_n^2. It can be shown that

$$\int_0^\pi P_n^2(t)\,\mathrm{d}t = \int_0^\pi \prod_{1\leq k\leq n} \sin^2\left(t - \frac{k\pi}{n}\right) \mathrm{d}t = \frac{\pi}{2^{2n-1}}. \tag{8.61}$$

In Figure 8.1 we plot the normalized integral

$$I_6(n) = \frac{4^n}{2\pi} \int_0^\pi P_n^2(t)\,\mathrm{d}t. \tag{8.62}$$

A separate paper investigating these integrals in more detail is currently in progress.

8.9 Some special classes of cyclotomic and inverse cyclotomic polynomials

In this section, we explore special cyclotomic polynomials Φ_n and inverse cyclotomic polynomials Ψ_n when the parameter n is a product of few distinct primes. The motivation stems from the intricate structure exhibited by the coefficients of these polynomials, as seen already in the proof of Suzuki's theorem. Specifically, we investigate recursive techniques for determining the coefficients of cyclotomic and inverse cyclotomic polynomials.

The subsections that follow detail some definitions and results regarding the coefficients of these special classes of cyclotomic and inverse cyclotomic polynomials. The results presented here include both established and new findings, with particular attention given to the coefficients of cyclotomic polynomials when n represents products of two or three distinct primes. The new results concerning formulas for the coefficients of ternary cyclotomic and inverse cyclotomic polynomials presented in this section have been submitted for publication in [30].

An interesting application of formula (8.10) is inspired by Theorem 8.9, from which one can observe that the coefficient $c_k^{(n)}$ of Φ_n can be computed recursively as

$$c_k^{(n)} = -\frac{\varphi(n)}{k}\left[\frac{\mu\left(\frac{n}{\gcd(n,k)}\right)}{\varphi\left(\frac{n}{\gcd(n,k)}\right)} + \frac{\mu\left(\frac{n}{\gcd(n,k-1)}\right)}{\varphi\left(\frac{n}{\gcd(n,k-1)}\right)}c_1^{(n)} + \cdots + \frac{\mu\left(\frac{n}{\gcd(n,1)}\right)}{\varphi\left(\frac{n}{\gcd(n,1)}\right)}c_{k-1}^{(n)}\right]. \tag{8.63}$$

Using the multiplicative properties of the functions featuring in the right hand side of (8.63) it is easy to show that this formula is equivalent to one first published in [121] and which is also recalled in the survey [230]. Therefore, one can argue that the use of Von Sterneck's formula (8.10) for reinterpreting Ramanujan sums gives a short proof of a known recursive formula.

Combining formula (8.10) with Theorem 8.13, it follows that the coefficient $d_k^{(n)}$ of Ψ_n can be obtained recursively as

$$d_k^{(n)} = \frac{\varphi(n)}{k}\left[-\frac{\mu\left(\frac{n}{\gcd(n,k)}\right)}{\varphi\left(\frac{n}{\gcd(n,k)}\right)} + \frac{\mu\left(\frac{n}{\gcd(n,k-1)}\right)}{\varphi\left(\frac{n}{\gcd(n,k-1)}\right)}d_1^{(n)} + \cdots + \frac{\mu\left(\frac{n}{\gcd(n,1)}\right)}{\varphi\left(\frac{n}{\gcd(n,1)}\right)}d_{k-1}^{(n)}\right]. \tag{8.64}$$

To complement the theoretical recurrence formula presented in (8.64), one can easily compute the coefficients of the n-th inverse cyclotomic polynomial using a computer algebra system such as Magma. By using a simple recursive approach, as outlined in the code snippet below, Magma can handle the necessary calculations, providing a practical form of these coefficients.

```
// Define the function to compute d_k^{(n)}
function InverseCyclotomicCoefficient(n, k)
    // Define the Euler totient function and the Mobius function
    phi := EulerPhi(n);
    mu_n := MoebiusMu(n);

    // Initialize the array to store the coefficients d_1^{(n)}, ..., d_k^{(n)}
    d := [0 : i in [1..k]];

    // Compute d_1^{(n)} = -mu(n)
    d[1] := -mu_n;

    // Recurrence to compute d_i^{(n)} for i >= 2
    for i in [2..k] do
        // Start with the first term
        gcd_ni := GCD(n, i);
        mu_term_i := MoebiusMu(n div gcd_ni);
        phi_term_i := EulerPhi(n div gcd_ni);

        // k * d_k^{(n)} starts with the first term
        i_di := - (phi / phi_term_i) * mu_term_i;

        // Add the sum for j = 1 to i-1
        for j in [1..i-1] do
            gcd_nij := GCD(n, i-j);
            mu_term_ij := MoebiusMu(n div gcd_nij);  // M\"obius term for this
                gcd
            phi_term_ij := EulerPhi(n div gcd_nij);
            i_di +:= (phi / phi_term_ij) * mu_term_ij * d[j];  // Include M\"
                obius term
        end for;

        // Now compute d_i^{(n)} by dividing by i
        d[i] := i_di / i;
    end for;

    // Return the result for d_k^{(n)}
    return d[k];
end function;
```

Proposition 8.4. *Suppose $n = p_1 p_2 \dots p_r$, where $p_1 < p_2 < \dots < p_r$ are primes. Then the first $p_1 + 1$ coefficients of the n-th cyclotomic polynomial belong to the set $\{-1, 0, 1\}$.*

Proof. In fact, we show that we can compute these coefficients. The results will differ, according to the parity of r.

From the formula (8.63), we have that if $1 \leq k < p_1 - 1$ then

$$c_k^{(n)} = \frac{(-1)^{r+1}}{k} \left[1 + c_1^{(n)} + \dots + c_{k-1}^{(n)} \right].$$

Note that $c_1^{(n)} = -\mu(n) = (-1)^{r+1}$.

If r is even, then $c_1^{(n)} = -1$ and hence $c_2^{(n)} = 0$. Inductively, one can use the same recurrence formula to show that $c_k^{(n)} = 0$, for all $2 \leq k \leq p_1 - 1$. Using the same formula, we have that

$$c_{p_1}^{(n)} = \frac{1}{p_1} \left[\varphi(p_1)(-1)^r + (-1)^{r+1} c_1^{(n)} + \dots + (-1)^{r+1} c_{p_1-1}^{(n)} \right],$$

hence $c_{p_1}^{(n)} = \frac{1}{p_1}(p_1 - 1 + 1) = 1$. Similarly, applying the recurrence formula again, one shows that $c_{p_1+1}^{(n)} = -1$.

When r is odd, the same recurrence formula and idea can be used to show that $c_k^{(n)} = 1$, for all $1 \leq k \leq p_1 - 1$, and that $c_{p_1}^{(n)} = c_{p_1+1}^{(n)} = 0$. □

For square-free values of n, we have the following analogous result for the coefficients of the inverse cyclotomic $d_k^{(n)}$ polynomials.

Proposition 8.5. *Let $n = p_1 p_2 \dots p_r$, where $p_1 < p_2 < \dots < p_r$ are primes. Then the first $p_1 + 1$ coefficients of the n-th inverse cyclotomic polynomial belong to the set $\{-1, 0, 1\}$.*

Proof. The proof follows the same lines as the one for Proposition 8.4. First we note that $d_1^{(n)} = -\mu(n) = (-1)^{r+1}$, for such n. Now, we distinguish the following two cases.

If r is odd and $p_1 > 2$, then from the recurrence formula (8.64) we compute $d_2^{(n)} = 0$. Now, inductively using the same recurrence formula it follows that $d_k^{(n)} = 0$ for all $2 \leq k \leq p_1 - 1$. By same recurrence formula, one sees that

$$d_{p_1}^{(n)} = -\frac{1}{p_1}(p_1 - 1 + 1 + 0 + \dots + 0) = -1.$$

To compute $d_{p_1+1}^{(n)}$ we directly apply the formula (8.64). First, we note that for such chosen n, we have $\mu(n) = -1$, $\mu(n/p_1) = 1$, $\gcd(n, p_1 + 1) = 1$, $\gcd(n, p_1) = p_1$ and $\gcd(n, k) = 1$ for all $1 \leq k \leq p - 1$. We get

$$d_{p_1+1}^{(n)} = \frac{1}{p_1 + 1}\left[1 + \varphi(p_1) - \underbrace{0 - \dots - 0}_{p-2 \text{ terms}} + 1\right] = 1.$$

Similarly, when r is even, one can compute that $d_1^{(n)} = -1$, $d_2^{(n)} = -1$. Then, inductively, as in the proof of the previous proposition, one can show that $d_k^{(n)} = -1$ for all $1 \leq k \leq p_1 - 1$. Moreover, $d_{p_1}^{(n)} = d_{p_1+1}^{(n)} = 0$. □

8.9.1 Coefficients of binary cyclotomic polynomials

Suppose $n = pq$, where $p < q$ are distinct primes. In this case, the polynomials Φ_n are said to be **binary** and has the following expression

$$\Phi_{pq}(z) = \frac{(z^{pq} - 1)(z - 1)}{(z^p - 1)(z^q - 1)}.$$

We note that our result in Proposition 8.4 implies that the first the first $p+1$ coefficients of this polynomial belong to the set $\{-1,0,1\}$.

Let u be the unique integer such that $0 < u < p$ and $uq \equiv -1 \pmod{p}$. Carlitz [87] showed that the number of positive coefficients of $\Phi_{pq}(z)$ is

$$\frac{(p-u)(uq+1)}{p}.$$

The following result about their coefficients is well-known and a proof can be found, for instance, in [166].

Theorem 8.19. *For $n = pq$, where $p < q$ are primes, write r,s for the unique positive integers such that $\varphi(n) = (p-1)(q-1) = pr - qs$. Then the coefficients of Φ_n are given by the following formulas*

$$c_k^{(n)} = \begin{cases} 1, \text{ if and only if } k = ip + jq \text{ with } i \in [0,r], j \in [0,s]; \\ -1, \text{ if and only if } k = ip + jq - pq, i \in [r+q, q-1], j \in [s+1, p-1]; \\ 0, \text{ otherwise.} \end{cases}$$

As the polynomial coefficients are 0, -1 and 1, they are called **flat**.

8.9.2 Coefficients of ternary polynomials Φ_n

We present the formula (8.63) in the special case when $n = pqr$, is a product of three distinct primes $p < q < r$. In this case, the polynomial Φ_n is called **ternary** and has the following apparently simple form

$$\Phi_{pqr}(z) = \frac{(1-z^{pqr})(1-z^r)(1-z^q)(1-z^p)}{(1-z^{qr})(1-z^{pr})(1-z^{pq})(1-z)}.$$

If $k < p$, then $\gcd(n,j) = 1$ for all $1 \le j \le k$, hence formula (8.63) becomes

$$c_k^{(n)} = \frac{1}{k}\left[1 + c_1^{(n)} + \cdots + c_{k-1}^{(n)}\right]. \tag{8.65}$$

For $k = p$, we have

$$c_p^{(n)} = \frac{1}{p}\left[-p + 1 + c_1^{(n)} + \cdots + c_{p-1}^{(n)}\right]. \tag{8.66}$$

By the two relations above, we prove the following result by induction.

Proposition 8.6. *Suppose $n = pqr$, where $p < q < r$ are primes. Then*

1. $c_k^{(n)} = 1$, *for all* $1 \le k \le p-1$;
2. $c_p^{(n)} = c_{p+1}^{(n)} = 0$.

Proof. Indeed, in this case we know that $c_1^{(n)} = -\mu(n) = 1$. Now, we prove the first claimed result using strong induction on k. Suppose $c_j^{(n)} = 1$ for all $1 \leq j \leq k$, where $k \leq p-2$. Then, using the recurrence in (8.65), we get that

$$c_{k+1}^{(n)} = \frac{1}{k+1}\left[1 + c_1^{(n)} + \ldots + c_k^{(n)}\right] = \frac{1}{k+1} \cdot (k+1) = 1$$

completing the induction.

Using what we just proved in (8.66) we obtain

$$c_p^{(n)} = \frac{1}{p}\left[-p+1+c_1^{(n)} + \cdots + c_{p-1}^{(n)}\right] = \frac{1}{p} \cdot (-p+1+p-1) = 0.$$

To compute the $(p+1)$-th coefficient of this polynomial, we will apply directly (8.63). Note that $\gcd(n, p+1) = 1$, $\gcd(n,p) = p$ and $\gcd(n,k) = 1$ for all $1 \leq k \leq p-1$. Also, in our hypotheses $\mu(n) = -1$ and $\mu(qr) = 1$. Plugging all these in the aforementioned formula, we obtain

$$c_{p+1}^{(n)} = -\frac{\varphi(n)}{p+1}\left[-\frac{1}{\varphi(n)} + \frac{1}{\varphi(qr)}c_1^{(n)} - \frac{1}{\varphi(n)}c_2^{(n)} \ldots - \frac{1}{\varphi(n)}c_{p-1}^{(n)} - \frac{1}{\varphi(n)}c_p^{(n)}\right],$$

which after replacing the previously known coefficients gives

$$c_{p+1}^{(n)} = -\frac{1}{p+1}\left[-(p-1) + \varphi(p)\right] = 0,$$

completing the proof of the second claim. □

In general, for $1 \leq j \leq k$, we have $\gcd(n, k-j) \in \{1, p, q, r, pq, rp, qr\}$, because $k \leq n - \varphi(n) < n$. Upon substituting the required values for φ and considering that $\mu(n) = -1$, $\mu(p) = \mu(q) = \mu(r) = -1$, and $\mu(pq) = \mu(pr) = \mu(qr) = 1$, we derive the formula

$$\begin{aligned} c_k^{(n)} = &-\frac{(p-1)(q-1)(r-1)}{k} \frac{\mu\left(\frac{n}{\gcd(n,k)}\right)}{\varphi\left(\frac{n}{\gcd(n,k)}\right)} + \frac{1}{k}\sum_{\gcd(n,k-j)=1} c_j^{(n)} \\ &- \frac{p-1}{k}\sum_{\gcd(n,k-j)=p} c_j^{(n)} - \frac{q-1}{k}\sum_{\gcd(n,k-j)=q} c_j^{(n)} - \frac{r-1}{k}\sum_{\gcd(n,k-j)=r} c_j^{(n)} \\ &+ \frac{(p-1)(q-1)}{k}\sum_{\gcd(n,k-j)=pq} c_j^{(n)} + \frac{(p-1)(r-1)}{k}\sum_{\gcd(n,k-j)=pr} c_j^{(n)} \\ &+ \frac{(q-1)(r-1)}{k}\sum_{\gcd(n,k-j)=qr} c_j^{(n)}, \end{aligned} \tag{8.67}$$

where all the sums above run through the values $1 \leq j \leq k-1$ satisfying the given condition regarding the greatest common divisor.

In what follows, we introduce the definition of a particular triple of prime numbers that will be used throughout the paper.

Definition 8.4. We call a triple of natural numbers (p,q,r) a Ramanujan triple if p,q,r are primes and $p < q < r < 2p$.

In his landmark 1919 paper [222], Ramanujan presented a novel proof of Bertrand's postulate, together with a generalisation. An important consequence is that for all $x \geq 11$ one has

$$\pi(x) - \pi\left(\frac{x}{2}\right) \geq 3,$$

where π represents the prime-counting function. By considering arbitrarily large values of x, there exist infinitely many distinct Ramanujan triples.

We note that for $n = pqr$, where (p,q,r) forms a Ramanujan triple, the recurrence formula above simplifies significantly, allowing us to obtain the following results, complementing the ones obtained in Proposition 8.6.

Proposition 8.7. *For every $n = pqr$ where (p,q,r) is a Ramanujan triple, we have*

1. $c_k^{(n)} = 0$ *for every* $p < k < q$;
2. $c_k^{(n)} = -1$ *for every* $q \leq k < r$;
3. $c_r^{(n)} = -2$.

Proof. We start by noting that for $p < k < q$ we have $\gcd(n, k-j) = 1$ for all $j \in \{1,2,\ldots,k-1\} \setminus \{k-p\}$. Morover, $\gcd(n,p) = p$. Using Proposition 8.6 in formula (8.63) we get

$$\begin{aligned} c_k^{(n)} &= -\frac{\varphi(n)}{k}\left[-\frac{k-p}{\varphi(n)} + \frac{p-1}{\varphi(n)} \cdot c_{k-p}^{(n)} - \frac{1}{\varphi(n)} \sum_{j=k-p+1}^{k-1} c_j^{(n)}\right] \\ &= -\frac{\varphi(n)}{k}\left[\frac{2p-1-k}{\varphi(n)} + \frac{k+1-2p}{\varphi(n)} - \frac{1}{\varphi(n)} \sum_{j=p}^{k-1} c_j^{(n)}\right] \\ &= \frac{1}{k} \sum_{j=p}^{k-1} c_j^{(n)}. \end{aligned}$$

Remark that in the second equality we used the fact that $k < q < 2p$ implies $0 < k-p < p$, hence $c_{k-p}^{(n)} = 1$. Now, we saw in Proposition 8.6 that $c_p^{(n)} = 0$. The formula above implies that $c_k^{(n)} = 0$ for all $p < k < q$, completing the proof of the first claim.

By the same argument, one can also compute the coefficient

$$\begin{aligned} c_q^{(n)} &= -\frac{\varphi(n)}{q}\left[\frac{\varphi(q)}{\varphi(n)} - \frac{1}{\varphi(n)}\sum_{k=1}^{q-p-1} c_k^{(n)} + \frac{\varphi(p)}{\varphi(n)} c_{q-p}^{(n)} - \sum_{k=q-p+1}^{q-1} c_k^{(n)}\right] \\ &= -\frac{1}{q}\left[(q-1)+(p+1)-q+(p-1) - \sum_{k=q-p+1}^{p-1} 1 - \underbrace{\sum_{k=p}^{q-1} c_k^{(n)}}_{=0}\right] \\ &= -\frac{1}{q}\cdot q = -1. \end{aligned}$$

We now compute the terms $c_k^{(n)}$ where $q < k < r$. By formula (8.63) we get

$$\begin{aligned} c_k^{(n)} &= -\frac{1}{k}\left[(-1)\sum_{j=0}^{k-q-1} 1 + \varphi(q) + (-1)\sum_{j=k-q+1}^{k-p-1} 1 + \varphi(p) + (-1)\sum_{j=k-p+1}^{p-1} 1 + \right. \\ &\quad \left. + (-1)\sum_{j=p}^{q-1} c_j^{(n)} + (-1)\sum_{j=q}^{k-1} c_j^{(n)}\right] \\ &= -\frac{1}{k}\left(q-k+q-1+p+1-q+p-1+k+1-2p - \sum_{j=q}^{k-1} c_j^{(n)}\right) \\ &= -\frac{1}{k}\left(q - \sum_{j=q}^{k-1} c_j^{(n)}\right). \end{aligned}$$

Now since we saw that $c_q^{(n)} = -1$, we obtain $c_k^{(n)} = -1$ for all $q < k < r$, which proves the second claim.

Similarly, we will compute the coefficient $c_r^{(n)}$ and for such n. We obtain

$$\begin{aligned} c_r^{(n)} &= -\frac{1}{r}\left[\varphi(r) + (-1)\sum_{j=1}^{r-q-1} 1 + \varphi(q) + (-1)\sum_{j=r-q+1}^{r-p-1} 1 + \varphi(p)\right. \\ &\quad \left. + (-1)\sum_{j=r-p+1}^{p-1} 1 + (-1)\sum_{j=p}^{q-1} 0 + (-1)\sum_{j=q}^{r-1}(-1)\right] = -\frac{1}{r}\cdot 2r = -2. \end{aligned}$$

This ends the proof. □

By Ramanujan's result, there is an infinite family of $n = pqr$ for which $c_r^{(n)} = -2$. While the first Ramanujan triple is $(7,11,13)$, where $n = 1001$, this polynomial has $c_{13}^{(1001)} = -2$ and $c_{199}^{(1001)} = -2$. but the polynomial has no coefficients of absolute value strictly greater than 2. However, for the Ramanujan triple $(17,19,29)$ and $n = 9367$ there are coefficients of larger absolute value such as $c_{3107}^{(9367)} = -4$.

8.9.3 Coefficients of binary inverse cyclotomic polynomials

Let us suppose that $n = pq$, where $p < q$ are primes. We discussed previously that in this case the polynomial Ψ_n is called binary. From the proof of the Proposition 8.5 we see that in this case $d_k^{(n)} = -1$ for all $1 \leq k \leq p-1$, and that $d_p^{(n)} = d_{p+1}^{(n)} = 0$. In this situation, the inverse cyclotomic polynomial has the following simple form

$$\Psi_n(z) = \frac{(z^p - 1)(z^q - 1)}{z - 1},$$

which is in turn equal to

$$\Psi_n(z) = z^{p+q-1} + \cdots + z^q - z^{p-1} - \cdots - z^2 - z - 1.$$

Hence, all the coefficients of these polynomials belong to the set $\{-1, 0, 1\}$, that is, the binary inverse cyclotomic polynomials are flat.

8.9.4 Coefficients of ternary inverse cyclotomic polynomials

As subsection 8.8.2, suppose $n = pqr$, where $p < q < r$ are primes. In this case, the polynomial Ψ_n is said to be **ternary** and has the following form

$$\Psi_n(z) = \frac{(z^{pq} - 1)(z^{qr} - 1)(z^{rp} - 1)(z - 1)}{(z^p - 1)(z^q - 1)(z^r - 1)}.$$

Despite its seemingly simple form, the structure of the coefficients of this polynomial remains quite intricate and is not yet fully understood.

If $k < p$, then $\gcd(n, j) = 1$ for all $1 \leq j \leq k$, hence formula (8.64) becomes

$$d_k^{(n)} = -\frac{1}{k}\left[-1 + d_1^{(n)} + \cdots + d_{k-1}^{(n)}\right]. \tag{8.68}$$

For $k = p$, we have

$$d_p^{(n)} = -\frac{1}{p}\left[p - 1 + d_1^{(n)} + \cdots + d_{p-1}^{(n)}\right]. \tag{8.69}$$

Building upon the recursive formula (8.64), we derive explicit formulas for the coefficients of Ψ_n. In particular, we find exact values of the coefficients $d_k^{(n)}$ up to the $(p+1)$-th term. This result is analogue to Proposition 8.6, where we previously determined the corresponding coefficients for the cyclotomic polynomial Φ_n.

We show that the coefficients of Ψ_n start with $d_1^{(n)} = 1$, and continue with the specific values of $d_k^{(n)}$ for $2 \leq k \leq p+1$.

Proposition 8.8. *Suppose $n = pqr$, where $p < q < r$ are primes. Then*

1. *$d_1^{(n)} = 1$ and $d_k^{(n)} = 0$, for all $2 \leq k \leq p-1$;*
2. *$d_p^{(n)} = -1$ and $d_{p+1}^{(n)} = 1$.*

Proof. The steps are similar to Proposition 8.6. First note that $d_1^{(n)} = -\mu(n) = 1$, for such n. By using (8.68), we get $d_2^{(n)} = -1/2\,(-1+1) = 0$. Now, the fact that $d_k^{(n)} = 0$, for all $2 \leq k \leq p-1$ follows from an immediate inductive argument and the same recurrence formula. Using (8.69) we get

$$d_p^{(n)} = -\frac{1}{p}\,[p-1+1+0+\cdots+0] = -1,$$

proving the third claim.

To compute $d_{p+1}^{(n)}$ we directly apply the formula (8.64). First, we note that for such chosen n, we have $\mu(n) = -1$, $\mu(n/p) = 1$, $\gcd(n, p+1) = 1$, $\gcd(n,p) = p$ and $\gcd(n,k) = 1$ for all $1 \leq k \leq p-1$. We get

$$d_{p+1}^{(n)} = \frac{\varphi(n)}{p+1}\left[\frac{1}{\varphi(n)} + \frac{1}{\varphi(qr)}d_1^{(n)} - \frac{1}{\varphi(n)}d_2^{(n)} - \ldots - \frac{1}{\varphi(n)}d_{p-1}^{(n)} - \frac{1}{\varphi(n)}d_p^{(n)}\right],$$

so

$$d_{p+1}^{(n)} = \frac{1}{p+1}\left[1 + \varphi(p) - \underbrace{0 - \ldots - 0}_{p-2 \text{ terms}} + 1\right] = 1,$$

completing the proof of the last claim. □

In general, for $1 \leq j \leq k$, we have $\gcd(n,j) \in \{1, p, q, r, pq, rp, qr\}$, because $k \leq n - \varphi(n) < n$, hence using that $\mu(n) = -1$, $\mu(p) = \mu(q) = \mu(r) = -1$, $\mu(pq) = \mu(pr) = \mu(qr) = 1$, we derive

$$\begin{aligned} d_k^{(n)} = &-\frac{(p-1)(q-1)(r-1)}{k}\,\frac{\mu\left(\frac{n}{\gcd(n,k)}\right)}{\varphi\left(\frac{n}{\gcd(n,k)}\right)} - \frac{1}{k}\sum_{\gcd(n,j)=1} d_j^{(n)} \\ &+ \frac{p-1}{k}\sum_{\gcd(n,j)=p} d_j^{(n)} + \frac{q-1}{k}\sum_{\gcd(n,j)=q} d_j^{(n)} + \frac{r-1}{k}\sum_{\gcd(n,j)=r} d_j^{(n)} \\ &- \frac{(p-1)(q-1)}{k}\sum_{\gcd(n,j)=pq} d_j^{(n)} - \frac{(p-1)(r-1)}{k}\sum_{\gcd(n,j)=pr} d_j^{(n)} \\ &- \frac{(q-1)(r-1)}{k}\sum_{\gcd(n,j)=qr} d_j^{(n)}, \end{aligned} \tag{8.70}$$

where all the sums above run through the values $1 \leq j \leq k-1$ satisfying the given condition regarding the greatest common divisor.

When (p,q,r) is a Ramanujan triple and $n = pqr$, formula (8.70) can be simplified. The following result complements Proposition 8.8.

Proposition 8.9. *For every $n = pqr$ where (p,q,r) is a Ramanujan triple, we have*

1. $d_k^{(n)} = 0$ *for all* $p+2 \leq k \leq q-1$ *and* $d_q^{(n)} = -1$;
2. $d_{q+1}^{(n)} = 1$ *and* $d_k^{(n)} = 0$ *for all* $q+2 \leq k < r$;
3. $d_r^{(n)} = -1$.

Proof. We saw above that $d_1^{(n)} = 1$, $d_k^{(n)} = 0$ for all $2 \leq k \leq p-1$, $d_p^{(n)} = -1$ and $d_{p+1}^{(n)} = 1$. If $p+1 < k < q$, then we have

$$d_k^{(n)} = \frac{1}{k}\left[1 + (-1) - d_p^{(n)} - d_{p+1}^{(n)} - \sum_{j=p+2}^{k-1} d_j\right] = \frac{1}{k}\sum_{j=p+2}^{k-1} d_j^{(n)},$$

which implies that $d_k^{(n)} = 0$ for all $p+2 \leq k \leq q-1$.

Similarly, for $k = q$ one shows that

$$d_q^{(n)} = \frac{1}{q}\left[-\varphi(q) + (-1) + (-1)\sum_{j=p}^{q-1} d_j^{(n)}\right] = \frac{1}{q}(1-q-1) = -1,$$

completing the proof of the first statement. To justify the second equality we note that all but the first two terms in the sum are equal to 0.

Similarly, it is easy to show that $d_{q+1}^{(n)} = 1$. When $q+2 \leq k < r$, one gets $d_k^{(n)} = \frac{1}{k}\left[\sum_{j=q+2}^{k} d_k^{(n)}\right]$ which is equal to 0, confirming the second statement.

Finally, when $k = r$ one obtains

$$\begin{aligned} d_r^{(n)} &= \frac{1}{r}\left[-\varphi(r) + (-1) + (-1)d_p^{(n)} + (-1)d_{p+1}^{(n)} + (-1)d_q^{(n)} + (-1)d_{q+1}^{(n)}\right] \\ &= \frac{1}{r}(-r+1-1) = -1. \end{aligned}$$

This ends the proof. □

We note that, combined with Ramanujan's result on the infinitude of such triples, Propositions 8.8 and 8.9 give precise values for the first r terms in an infinite family of inverse cyclotomic polynomials. One would be mislead to think that for $n = pqr$, where (p,q,r) is a Ramanujan triple, the inverse cyclotomic polynomials are flat. Indeed, when $n = 11 \cdot 13 \cdot 19$, the computations implemented in Magma confirmed that $d_{53}^{(n)} = 2$. Similar computations were carried out for the Ramanujan triple $(101,103,109)$ and $n = 1133927$ where we calculated that $d_{15651}^{(n)} = -16$.

8.9.5 Numerical simulations

In this section, we present numerical simulations for two specific cases of interest, namely the 105-th cyclotomic polynomial Φ_{105} and the 561-th inverse cyclotomic polynomial Ψ_{561}, the first instances where the polynomials are non-flat. The goal of the following subsections is to illustrate, step by step, how the first non-flat coefficients can be computed for each polynomial using the recurrence formulas and methods discussed in the previous section. These computations provide insight into the structure of the coefficients and suggest a pattern for how larger coefficients tend to concentrate toward the center of the polynomials.

8.9.5.1 Results for Φ_{105}

When $n = 3 \cdot 5 \cdot 7 = 105$, we have $c_1^{(n)} = -\mu(n) = 1$ and from Proposition 8.6, we know that $c_2^{(n)} = 1$, $c_3^{(n)} = 0$.

Now, using the recurrence formula (8.63) we obtain

$$\begin{aligned} c_4^{(n)} &= -\frac{\varphi(105)}{4}\left[\frac{\mu(105)}{\varphi(105)} + \frac{\mu(5\cdot 7)}{\varphi(5\cdot 7)}c_1^{(n)} + \frac{\mu(105)}{\varphi(105)}c_2^{(n)} + \frac{\mu(105)}{\varphi(105)}c_3^{(n)}\right] \\ &= -\frac{1}{4}\left[-1 + 2\cdot 1 - 1\cdot 1 - 1\cdot 0\right] = 0. \end{aligned}$$

Similarly, $c_5^{(n)} = -1$ and $c_6^{(n)} = -1$. Now, we use the formula to get

$$\begin{aligned} c_7^{(n)} &= -\frac{\varphi(105)}{7}\left[\frac{\mu(15)}{\varphi(15)} + \frac{\mu(35)}{\varphi(35)}\cdot c_1^{(n)} + \frac{\mu(21)}{\varphi(21)}\cdot c_2^{(n)} + \frac{\mu(105)}{\varphi(105)}\cdot c_3^{(n)}\right. \\ &\quad \left. + \frac{\mu(35)}{\varphi(35)}\cdot c_4^{(n)} + \frac{\mu(105)}{\varphi(105)}\cdot c_5^{(n)} + \frac{\mu(105)}{\varphi(105)}\cdot c_6^{(n)}\right] \\ &= -\frac{1}{7}\left[6 + 2\cdot 1 + 4\cdot 1 + (-1)\cdot 0 + 2\cdot 0 + (-1)\cdot(-1) + (-1)\cdot(-1)\right] \\ &= -2. \end{aligned}$$

This confirms that -2 appears as the coefficient of z^7 in

$$\begin{aligned} \Phi_{105}(z) = {} & z^{48} + z^{47} + z^{46} - z^{43} - z^{42} - 2z^{41} - z^{40} - z^{39} + z^{36} + z^{35} + z^{34} \\ & + z^{33} + z^{32} + z^{31} - z^{28} - z^{26} - z^{24} - z^{22} - z^{20} + z^{17} + z^{16} + z^{15} \\ & + z^{14} + z^{13} + z^{12} - z^9 - z^8 - 2z^7 - z^6 - z^5 + z^2 + z + 1. \end{aligned}$$

While this result is aligned with Proposition 8.7.3 stating that $c_r^{(n)} = -2$, we notice that $(p,q,r) = (3,5,7)$ is not a Ramanujan triple.

8.9.5.2 Results for Ψ_{561}

For numerical simulations we focus on some instances where Ψ_n is not flat. It is known that the first non flat inverse cyclotomic polynomial is Ψ_{561}. As listed in Table 1 of [204], -3 first appears in Ψ_{1155} as the coefficient of z^{33}, while 4 first appears in Ψ_{2145} as the coefficient of z^{44}. These are the three cases we focus on, and we compute explicitly until we get the first coefficient which is not 0, 1 or -1.

Let us focus on the case $n = 561 = 3 \cdot 11 \cdot 17$.

Since $\mu(n) = -1$, by the argument used earlier we get $d_1^{(n)} = -\mu(n) = 1$. From Proposition 8.8 we have $d_2^{(n)} = 0$ and $d_3^{(n)} = -1$, so by (8.64), we get

$$\begin{aligned} d_4^{(n)} &= \frac{\varphi(561)}{4}\left[-\frac{\mu(561)}{\varphi(561)} + \frac{\mu(187)}{\varphi(187)} \cdot d_1^{(n)} + \frac{\mu(561)}{\varphi(561)} \cdot d_2^{(n)} + \frac{\mu(561)}{\varphi(561)} \cdot d_3^{(n)}\right] \\ &= \frac{1}{4}\left[1 + 2 \cdot 1 + (-1) \cdot 0 + (-1) \cdot (-1)\right] = 1; \end{aligned}$$

Similarly, one obtains can compute $d_5^{(n)} = 0$, $d_6^{(n)} = -1$, $d_7^{(n)} = 1$, $d_8^{(n)} = 0$, $d_9^{(n)} = -1$, $d_{10}^{(n)} = 1$, $d_1 1^{(n)} = -1$, $d_{12}^{(n)} = 0$, $d_{13}^{(n)} = 1$, $d_{14}^{(n)} = -1$, $d_{15}^{(n)} = 0$, $d_{16}^{(n)} = 1$, from where

$$\begin{aligned} d_{17}^{(n)} &= \frac{1}{17}\left[-16 + (-1) \cdot 1 + 2 \cdot 0 + (-1) \cdot (-1) + (-1) \cdot 1 + 2 \cdot 0 + 10 \cdot (-1)\right] + \\ &+ \frac{1}{17}\left[(-1) \cdot 1 + 2 \cdot 0 + (-1) \cdot (-1) + (-1) \cdot 1 + 2 \cdot (-1) + (-1) \cdot 0\right] + \\ &+ \frac{1}{17}\left[(-1) \cdot 1 + 2 \cdot (-1) + (-1) \cdot 0 + (-1) \cdot 1\right] = -2; \end{aligned}$$

This confirms that -2 appears as the coefficient of z^{17} in

$$\begin{aligned} \Psi_{561}(z) = z^{241} - z^{240} + \cdots + 2z^{224} + \cdots + z^{18} + \\ - 2z^{17} + z^{16} - z^{14} + z^{13} - z^{11} + z^{10} - z^9 + z^7 - z^6 + z^4 - z^3 + z - 1. \end{aligned}$$

This argument allows the calculation of further coefficients, and suggests why the larger coefficients of inverse cyclotomic polynomials are moving towards the centre (also using the fact that the polynomial is antipalindromic).

Sincein Proposition 8.9.3 we had $d_r^{(n)} = -1$, so the condition that (p,q,r) is a Ramanujan triple is necessary, as $(3,11,17)$ is clearly not Ramanujan.

Chapter 9
Special Polynomials and their Coefficients

In this chapter we investigate some classes of polynomials defined by factorization, whose roots are situated on the unit circle with possible multiplicities. For these polynomials we establish integral formulae for the coefficients, which are useful in the study of certain asymptotic properties. We also study recurrence relations, connections to other classical polynomials, or associated integer sequences, recently added to the Online Encyclopedia of Integer Sequences (OEIS).

In Section 9.1 we define and study a general family of polynomials depending on an integer sequence $m_1,\ldots,m_n,\ldots$, and on a sequence of complex numbers $z_1,\ldots,z_n,\ldots$ of modulus one [20], for which we derive an integral formula for the coefficients.

In Section 9.2 we discuss some key results concerning the cyclotomic polynomials and their coefficients. These have numerous applications in discrete mathematics and number theory. The integral formulae for the coefficients of cyclotomic obtained in [20], are used to prove some classical results, or to study formulae for the direct or alternate sums of coefficients.

Section 9.3 is dedicated to the polygonal polynomials [17], which have applications in the study of integer partitions. We first present integral formulae and recurrence relations for the coefficients, then highlight combinatorial interpretations and connections to the Mahonian polynomials.

In Sections 9.4 and 9.5 are defined and investigated the extended cyclotomic polynomials, and the extended polygonal-type polynomials, respectively. For these polynomials we present integral formulae for the coefficients, links to partitions and some integer sequences.

Section 9.6 concerns the study of the multinomial, Gaussian and Catalan polynomials, based on [18]. The following two sections are dedicated to the extended cyclotomic, and extended polygonal-type polynomials, introduced in [19]. All these polynomials are recovered as particular instances of the general family of polynomials presented in Section 9.1.

9.1 A general class of polynomials

In this section we introduce a class of polynomials defined by an integer sequence $m_1,\dots,m_n,\dots$, and a sequence $z_1,\dots,z_n,\dots$, of complex numbers of modulus one, which recovers cyclotomic, polygonal, and multinomial polynomials as special cases.

9.1.1 Definition and basic properties

Consider the positive integers n, $m_1,\dots,m_n$, and the complex numbers $z_1,\dots,z_n$ with $|z_1| = \cdots = |z_n| = 1$. We define the polynomial

$$F_{m_1,\dots,m_n}^{z_1,\dots,z_n}(z) = \prod_{k=1}^{n}(z^{m_k} - z_k). \tag{9.1}$$

Clearly, the degree of $F_{m_1,\dots,m_n}^{z_1,\dots,z_n}(z)$ is $m_1 + \cdots + m_n$. While this polynomial is factorized as a product of factors $z - \zeta$, where $|\zeta| = 1$, this form is not practical. The product of absolute values of the roots is one, hence the Mahler measure of $F_{m_1,\dots,m_n}^{z_1,\dots,z_n}$ is 1. An interesting and challenging problem is to find reasonable formulae for the coefficients after multiplication.

Numerous interesting polynomials are obtained for particular choices of the sequences $m_1,\dots,m_n,\dots$ and $z_1,\dots,z_n,\dots$. Some of them are explored in some detail throughout this chapter.

9.1.2 Integral formulae for the coefficients

In what follows we obtain an integral formula for the coefficients of $F_{m_1,\dots,m_n}^{z_1,\dots,z_n}$. The method we use is a special case of the Cauchy integral formula (see [75]), adapted for complex polynomials, where the integration curve is the unit circle (see [19]). Denote $z_k = \cos\alpha_k + i\sin\alpha_k$, $k = 1,\dots,n$, $\alpha = \alpha_1 + \cdots + \alpha_n$, $m = m_1 + \cdots + m_n$, and consider $z = \cos 2t + i\sin 2t$ for $t \in [0,\pi]$.

To get a unified formula for the coefficients of the polynomial (9.1), it is useful to introduce the function

$$\Lambda(t;m_1,\dots,m_n;\alpha_1,\dots,\alpha_n) = \prod_{k=1}^{n}\sin\left(m_k t - \frac{\alpha_k}{2}\right), \quad t \in [0,\pi]. \tag{9.2}$$

For each $k = 1,\dots,n$, by computations involving Euler's exponential notation of complex numbers in polar form, we obtain:

$$\begin{aligned} z^{m_k} - z_k &= (\cos 2m_k t - \cos\alpha_k) + i\,(\sin 2m_k t - \sin\alpha_k) \\ &= 2i \sin\left(m_k t - \frac{\alpha_k}{2}\right) e^{i\left(m_k t + \frac{\alpha_k}{2}\right)}. \end{aligned} \tag{9.3}$$

Writing the polynomial $F^{z_1,\ldots,z_n}_{m_1,\ldots,m_n}$ in algebraic form, it follows that

$$\begin{aligned} F^{z_1,\ldots,z_n}_{m_1,\ldots,m_n}(z) &= \sum_{j=0}^{m} C_j z^j = \prod_{k=1}^{n} (z^{m_k} - z_k) \\ &= (2i)^n \prod_{k=1}^{n} \sin\left(m_k t - \frac{\alpha_k}{2}\right) e^{i\left(m_k t + \frac{\alpha_k}{2}\right)} \\ &= (2i)^n \Lambda(t; m_1, \ldots, m_n; \alpha_1, \ldots, \alpha_n) e^{i\left(mt + \frac{\alpha}{2}\right)}. \end{aligned} \tag{9.4}$$

Using the multiplication of complex numbers in polar form we deduce

$$\begin{aligned} C_j + \sum_{k \neq j} C_k z^{k-j} &= z^{-j} \prod_{k=1}^{n} (z^{m_k} - z_k) \\ &= z^{-j} (2i)^n \Lambda(t; m_1, \ldots, m_n; \alpha_1, \ldots, \alpha_n) e^{i\left(mt + \frac{\alpha}{2}\right)} \\ &= (2i)^n \Lambda(t; m_1, \ldots, m_n; \alpha_1, \ldots, \alpha_n) e^{i\left((m-2j)t + \frac{\alpha}{2}\right)}. \end{aligned}$$

Integrating the above relation over $[0, \pi]$, we get the following result.

Theorem 9.1. *(1) The coefficients of polynomial $F^{z_1,\ldots,z_n}_{m_1,\ldots,m_n}$ are given by*

$$C_j = \frac{(2i)^n}{\pi} \int_0^{\pi} \Lambda(t; m_1, \ldots, m_n; \alpha_1, \ldots, \alpha_n) e^{i\left((m-2j)t + \frac{\alpha}{2}\right)}\, \mathrm{d}t. \tag{9.5}$$

(2) If the coefficient C_j is a real number, then it is given by

$$\begin{cases} \frac{(-1)^{\frac{n}{2}} 2^n}{\pi} \int_0^{\pi} \Lambda(t; m_1, \ldots, m_n; \alpha_1, \ldots, \alpha_n) \cos\left((m-2j)t + \frac{\alpha}{2}\right) \mathrm{d}t & \text{if } n \text{ is even} \\ \frac{(-1)^{\frac{n+1}{2}} 2^n}{\pi} \int_0^{\pi} \Lambda(t; m_1, \ldots, m_n; \alpha_1, \ldots, \alpha_n) \sin\left((m-2j)t + \frac{\alpha}{2}\right) \mathrm{d}t & \text{if } n \text{ is odd.} \end{cases}$$

9.2 Polygonal polynomials

Here we explore properties of the polygonal polynomials P_n defined in [17]. A general framework based on the Cauchy's integral formula (Section 5.3) and applications to the study of k-partitions of multisets was given in [19]. We then study the coefficients of P_n, for which we establish a recursive formula , we deduce an exact integral formula and give a combinatorial interpretation. We then investigate connections to the Mahonian polynomials Q_n and present related integer sequences.

9.2.1 Definition and basic properties

The n-th **polygonal polynomial** was defined in [17], by

$$P_n(z) = (z-1)(z^2-1)\cdots(z^n-1) = \sum_{j=0}^{\frac{n(n+1)}{2}} c_j^{(n)} z^j. \tag{9.6}$$

The roots of P_n are the complex coordinates of the vertices, with repetitions, of the regular k-gons centered in the origin, and having 1 as a vertex, $k = 1,\ldots,n$, which justifies the name. These polynomials are closely linked to Euler's famous pentagonal number theorem concerning the infinite expansion $(1-x)(1-x^2)(1-x^3)\cdots = \sum_{k=-\infty}^{\infty}(-1)^k x^{k(3k-1)/2}$, where $|x|<1$, and the exponents are called (generalised) pentagonal numbers [42].

We recall that $z^n - 1 = \prod_{d|n}\Phi_d(z)$, hence the polynomial P_n can be decomposed as product of cyclotomic polynomials

$$P_n(z) = \prod_{k=1}^{n}\prod_{d|k}\Phi_d(z). \tag{9.7}$$

As every cyclotomic polynomial is irreducible over $\mathbb{Z}$ ([146], Thm. 1, p. 195), the polynomial P_n has exactly $\nu(n) = \sum_{k=1}^{n}\tau(k)$ factors irreducible over $\mathbb{Z}$, where $\tau(k)$ denotes the number of divisors of the positive integer k.

While the polynomial P_n seems simple, it exhibits deep algebraic, arithmetic and combinatorial properties. Its natural companion is the Mahonian polynomial Q_n defined in (9.16), with a key role in the theory of partitions.

9.2.1.1 Palindromicity of the coefficients of P_n

Recall that a polynomial $f(z) = a_0 + a_1 z + \cdots + a_m z^m$ of degree m is called

- **palindromic** (reciprocal) if $f(z) = z^m f\left(\frac{1}{z}\right)$, i.e., $a_j = a_{m-j}$, $j = 0,\ldots,m$;
- **antipalindromic** (antireciprocal) if $f(z) = -z^m f\left(\frac{1}{z}\right)$, i.e., $a_j = -a_{m-j}$;
- **unimodal** if the sequence of coefficients is unimodal, i.e., there is an integer t (called mode), with $a_1 \le a_2 \le \cdots \le a_t$ and $a_t \ge a_{t+1} \ge \cdots \ge a_m$.

Notice that

$$P_n(z) = (-1)^n z^{\frac{n(n+1)}{2}} P_n\left(\frac{1}{z}\right),$$

hence P_n is palindromic if n even, i.e., $c_j^{(n)} = c_{\frac{n(n+1)}{2}-j}^{(n)}$, $j = 0,\ldots,\frac{n(n+1)}{2}$, while P_n is antipalindromic for n odd, i.e., $c_j^{(n)} = -c_{\frac{n(n+1)}{2}-j}^{(n)}$, $j = 0,\ldots,\frac{n(n+1)}{2}$.

9.2.2 A recursive formula for coefficients

The coefficients of P_n can be obtained recursively, from

$$P_n(z) = \prod_{k=1}^{n} (z^k - 1) = P_{n-1}(z)\,(z^n - 1)\,.$$

Writing P_n and P_{n-1} explicitly, one obtains

$$\begin{aligned} P_n(z) &= \sum_{j=0}^{\frac{n(n+1)}{2}} c_j^{(n)} z^j \\ &= \left(\sum_{j=0}^{\frac{n(n-1)}{2}} c_j^{(n-1)} z^j \right) (z^n - 1)\,. \end{aligned}$$

This indicates the following formula:

$$c_j^{(n)} = \begin{cases} -c_j^{(n-1)} & \text{if } j \in \{0,\dots,n-1\}\,, \\ c_{j-n}^{(n-1)} - c_j^{(n-1)} & \text{if } j \in \left\{n,\dots,\frac{n(n-1)}{2}\right\}, \\ c_j^{(n-1)} & \text{if } j \in \left\{\frac{n(n-1)}{2}+1,\dots,\frac{n(n+1)}{2}\right\}. \end{cases} \tag{9.8}$$

Using the recurrence (9.8), we obtain the numbers in Table 9.1.

The values of the coefficients $c_j^{(n)}$ correspond to the sequence $(-1)^n T(n,j)$ indexed A231599 in the Online Encyclopedia of Integer Sequences [211].

9.2.3 Integral formulae for the coefficients

Setting $m_k = k$ and $z_k = 1$ for $k = 1,\dots,n$ in the polynomial (9.28), we obtain the polygonal polynomials P_n given in (9.6), investigated in our paper [17].

Also, the formula (9.2) where $\alpha_k = 0$, $k = 1,\dots,n$, is simply denoted by

$$\Lambda(t;1,\dots,n) = \prod_{k=1}^{n} \sin kt, \quad t \in [0,\pi], \tag{9.9}$$

while the degree of the polynomial P_n is

$$m = 1 + \cdots + n = \frac{n(n+1)}{2}.$$

By applying the results in Theorem 9.1 (2), it follows the integral formula

$c_j^{(1)}$	-1, 1
$P_1(z)$	$-1+z$
$c_j^{(2)}$	1, -1, -1, 1
$P_2(z)$	$1-z-z^2+z^3$
$c_j^{(3)}$	-1, 1, 1, 0, -1, -1, 1
$P_3(z)$	$-1+z+z^2-z^4-z^5+z^6$
$c_j^{(4)}$	1, -1, -1 , 0, 0, 2 , 0, 0, -1 , -1, 1
$P_4(z)$	$1-z-z^2+2z^5-z^8-z^9+z^{10}$
$c_j^{(5)}$	-1, 1, 1, 0, 0, -1, -1, -1, 1, 1, 1, 0, 0, -1, -1, 1
$P_5(z)$	$-1+z+z^2-z^5-z^6-z^7+z^8+z^9+z^{10}-z^{13}-z^{14}+z^{15}$
$c_j^{(6)}$	1, -1, -1, 0, 0, 1, 0, 2, 0, -1, -1, -1, -1, 0, 2, 0, 1, 0, 0, -1, -1, 1
$P_6(z)$	$1-z-z^2+z^5+2z^7-z^9-z^{10}-z^{11}-z^{12}+2z^{14}+z^{16}-z^{19}-z^{20}+z^{21}$
$c_j^{(7)}$	-1, 1, 1, 0, 0, -1, 0, -1, -1, 0, 1, 1, 2, 0, 0, 0, -2, -1, -1, 0, 1, 1, 0, 1, 0, 0, -1, -1, 1
$P_7(z)$	$-1+z+z^2-z^5-z^7-z^8+z^{10}+z^{11}+2z^{12}-2z^{16}-z^{17}-z^{18}+z^{20}+$ $+z^{21}+z^{23}-z^{26}-z^{27}+z^{28}$

Table 9.1 Polynomials P_n and their coefficients for $n = 1,2,3,4,5,6,7$.

$$c_j^{(n)} = \frac{2^n}{\pi}\int_0^\pi \cos\left(\frac{n(n+1)-4j}{2}t+\frac{n\pi}{2}\right)\sin t\sin 2t\cdots\sin nt\,\mathrm{d}t \tag{9.10}$$
$$= \begin{cases} \frac{(-1)^{\frac{n}{2}}2^n}{\pi}\int_0^\pi \cos\left(\frac{n(n+1)-4j}{2}t\right)\sin t\sin 2t\cdots\sin nt\,\mathrm{d}t & \text{if n is even} \\ \frac{(-1)^{\frac{n+1}{2}}2^n}{\pi}\int_0^\pi \sin\left(\frac{n(n+1)-4j}{2}t\right)\sin t\sin 2t\cdots\sin nt\,\mathrm{d}t & \text{if n is odd.} \end{cases}$$

9.2.4 The combinatorial interpretation of the coefficients

The calculation of these polynomial coefficients involves tuples with fixed sum. Let s,k,n be positive integers. We denote by $\alpha(s,k,n)$ the number of integer s-tuples $(i_1,\ldots,i_s)$ with the properties

$$i_1+i_2+\cdots+i_s = k, \quad 1\le i_1<i_2<\cdots<i_s\le n. \tag{9.11}$$

The link with the coefficients $c_j^{(n)}$ is given in the following theorem.

Theorem 9.2. *The following formula holds:*

$$c_k^{(n)} = (-1)^{n-1}\left(\alpha(1,k,n)-\alpha(2,k,n)+\alpha(3,k,n)-\cdots\right). \tag{9.12}$$

Proof. The coefficient $c_k^{(n)}$ of z^k in the expansion $(z-1)(z^2-1)\cdots(z^n-1)$ involves s distinct terms chosen from the set $\{1,\ldots,n\}$ with the property that their sum is k, and also $n-s$ terms equal to (-1), for $s=0,\ldots,n$. Explicitly, $c_k^{(n)}$ is given by the expression

$$c_k^{(n)} = (-1)^{n-1}\alpha(1,k,n) + (-1)^{n-2}\alpha(2,k,n) + (-1)^{n-3}\alpha(3,k,n) + \cdots.$$

This ends the proof. □

Clearly, $\alpha(s,k,n)$ is an increasing function with n. When n is large enough, the function is stationary to a value independent of n, denoted by $\alpha(s,k)$.

The following result links the polynomial P_s to $\alpha(s,k)$.

Theorem 9.3. *If s is a positive integer, then for all $z\in\mathbb{C}$ such that $|z|<1$ we have*

$$\frac{(-1)^s z^{\frac{s(s+1)}{2}}}{P_s(z)} = \lim_{n\to\infty} \sum_{1\le i_1<i_2<\cdots<i_s\le n} z^{i_1+i_2+\cdots+i_s} = \sum_{k=0}^{\infty}\alpha(s,k)z^k. \tag{9.13}$$

Proof. Clearly, we have

$$\begin{aligned}
&\lim_{n\to\infty}\sum_{1\le i_1<\cdots<i_s\le n} z^{i_1+\cdots+i_s} = \sum_{1\le i_1<\cdots<i_s} z^{i_1+\cdots+i_s}\\
&= \sum_{1\le i_1<\cdots<i_{s-1}} z^{i_1+\cdots+i_{s-1}}\cdot\frac{z^{i_{s-1}+1}}{1-z} = \frac{z}{1-z}\sum_{1\le i_1<\cdots<i_{s-1}} z^{i_1+\cdots+2i_{s-1}}\\
&= \frac{z}{1-z}\sum_{1\le i_1<\cdots<i_{s-2}} z^{i_1+\cdots+i_{s-2}}\cdot\frac{z^{2(i_{s-2}+1)}}{1-z^2}\\
&= \frac{z^{1+2}}{(1-z)(1-z^2)}\sum_{1\le i_1<\cdots<i_{s-2}} z^{i_1+\cdots+3i_{s-2}} = \cdots\\
&= \frac{z^{1+\cdots+(s-1)}}{(1-z)\cdots(1-z^{s-1})}\sum_{1\le i_1} z^{si_1} = \frac{z^{\frac{s(s+1)}{2}}}{(1-z)\cdots(1-z^s)}\\
&= \frac{(-1)^s z^{\frac{s(s+1)}{2}}}{P_s(z)}.
\end{aligned}$$

□

Notice also that by (9.13) it follows that

$$(-1)^s z^{\frac{s(s+1)}{2}} = P_s(z)\left(\sum_{k=0}^{\infty}\alpha(s,k)z^k\right) = \left(\sum_{j=0}^{\frac{s(s+1)}{2}} c_j^{(s)} z^j\right)\left(\sum_{k=0}^{\infty}\alpha(s,k)z^k\right),$$

hence we obtain the following result.

Corollary 9.1. *Considering that* $c_j^{(s)} = 0$ *for* $j > \frac{s(s+1)}{2}$, *we have*

$$\sum_{j=0}^{n} \alpha(s, n-j) c_j^{(s)} = (-1)^s \delta_{n, \frac{s(s+1)}{2}}, \tag{9.14}$$

where $\delta_{u,v}$ *denotes the Kronecker symbol.*

Corollary 9.2. *Let* $\beta(s,k)$ *be the number of distinct solutions to the equation*

$$j_1 + 2j_2 + \cdots + sj_s = k, \tag{9.15}$$

such that the numbers $j_1, j_2, \ldots, j_s \geq 1$ *may be equal. We have* $\alpha(s,k) = \beta(s,k)$.

Proof. Indeed, for $j \in \{1, \ldots, s\}$ and $|z| < 1$ one has $\dfrac{z^j}{1-z^j} = z^j + z^{2j} + \cdots$. By taking the product over $j \in \{1, \ldots, s\}$, one obtains

$$\frac{(-1)^s z^{\frac{s(s+1)}{2}}}{P_s(z)} = (z + z^2 + \cdots) \cdots (z^s + z^{2s} + \cdots) = \sum_{k=0}^{\infty} \beta(s,k) z^k.$$

The result follows by (9.13). Clearly, $\alpha(s,k) = \beta(s,k) = 0$ for $0 \leq k \leq \frac{s(s+1)}{2} - 1$.

Results counting the ordered partitions of the integer k into s parts each of size at least 0 but no larger than n have been obtained in [223] and [247]. □

9.2.5 The connection to the Mahonian polynomial Q_n

The polygonal polynomial can be written as $P_n(z) = (z-1)^n Q_n(z)$, where

$$Q_n(z) = (z+1) \cdots (z^{n-1} + z^{n-2} + \cdots + z + 1) = \sum_{j=0}^{\frac{(n-1)n}{2}} a_j^{(n)} z^j. \tag{9.16}$$

We call Q_n the Mahonian polynomial, which presents interest in its own right and has been investigated in many papers (see, e.g., [190] or [205]). The coefficients $a_k^{(n)}$ are called Mahonian numbers, representing the number of permutations of $\{1, \ldots, n\}$ with k inversions, indexed as A008302 in OEIS.

If $z^k = z^{k_1} \cdots z^{k_{n-1}}$ with z^{k_j} coming from the factor $1 + z + \cdots + z^j$ in (9.16), then an interpretation of the coefficient $a_k^{(n)}$ is the number of partitions of the integer $k = k_1 + \cdots + k_{n-1}$, with the constraints $0 \leq k_j \leq j, \quad 1 \leq j \leq n-1$. These numbers are related to the Mahonian distribution, which interestingly, are used in the mixing of diffusing particles [65].

$a_j^{(2)}$	$1, 1$
$Q_2(z)$	$1+z$
$a_j^{(3)}$	$1, 2, 2, 1$
$Q_3(z)$	$1+2z+2z^2+z^3$
$a_j^{(4)}$	$1, 3, 5, 6, 5, 3, 1$
$Q_4(z)$	$1+3z+5z^2+6z^3+5z^4+3z^5+z^6$
$a_j^{(5)}$	$1, 4, 9, 15, 20, 22, 20, 15, 9, 4, 1$
$Q_5(z)$	$1+4z+9z^2+15z^3+20z^4+22z^5+20z^6+15z^8+9z^8+4z^9+z^{10}$
$a_j^{(6)}$	$1, 5, 14, 29, 49, 71, 90, 101, 101, 90, 71, 49, 29, 14, 5, 1$
$Q_6(z)$	$1+5z+14z^2+29z^3+49z^4+71z^5+90z^6+101z^7+101z^8+90z^9+$ $71z^{10}+49z^{11}+29z^{12}+14z^{13}+5z^{14}+z^{15}$

Table 9.2 Polynomials Q_n and their coefficients for $n = 2,3,4,5,6$.

For $n = 10$ the following formula is obtained for the polynomial Q_{10}:

$$\begin{aligned}Q_{10}(z) = {} & 1+9z+44z^2+155z^3+440z^4+1068z^5+2298z^6+4489z^7+\\ & +8095z^8+13640z^9+21670z^{10}+32683z^{11}+47043z^{12}+\\ & +64889z^{13}+86054z^{14}+110010z^{15}+135853z^{16}+162337z^{17}+\\ & +187959z^{18}+211089z^{19}+230131z^{20}+243694z^{21}+250749z^{22}+\\ & +250749z^{23}+243694z^{24}+230131z^{25}+211089z^{26}+187959z^{27}+\\ & +162337z^{28}+135853z^{29}110010z^{30}+86054z^{31}+64889z^{32}+\\ & +47043z^{33}+32683z^{34}+21670z^{35}+13640z^{36}+8095z^{37}+\\ & +4489z^{38}+2298z^{39}+1068z^{40}+440z^{41}+\\ & +155z^{42}+44z^{43}+9z^{44}+z^{45}.\end{aligned}$$

We give a recursive formula for $a_j^{(n)}$, depending on the coefficients of Q_j.

Theorem 9.4. *Let $n \geq k+1$. The coefficient $a_k^{(n)}$ is given by the recursive formula*

$$a_k^{(n)} = \sum_{j=0}^{k} \binom{n-1-j}{k-j} a_j^{(k)}. \tag{9.17}$$

Proof. Clearly, $a_k^{(n)}$ is the coefficient of z^k in $Q_k(z)(1+z+\cdots+z^k)^{n-k}$, and

$$(1+z+\cdots+z^k)^{n-k} = \left(\frac{1-z^{k+1}}{1-z}\right)^{n-k} = \left(1-z^{k+1}\right)^{n-k}\left(\frac{1}{1-z}\right)^{n-k}.$$

For $|z| < 1$, the geometric series summation yields

$$\frac{1}{1-z} = 1 + z + z^2 + \cdots + z^s + \cdots.$$

By differentiating $(n-k-1)$ times one obtains

$$(n-k-1)!\left(\frac{1}{1-z}\right)^{n-k} = \sum_{s=0}^{\infty}(s+1)(s+2)\cdots(s+n-k-1)z^s,$$

hence

$$\left(\frac{1}{1-z}\right)^{n-k} = \sum_{s=0}^{\infty}\frac{(s+1)\cdots(s+n-k-1)}{(n-k-1)!}z^s = \sum_{s=0}^{\infty}\binom{s+n-1-k}{s}z^s.$$

The coefficient of z^k in

$$\left(\sum_{j=0}^{\frac{k(k-1)}{2}} a_j^{(k)}\right)\left(1-z^{k+1}\right)^{n-k}\left(\frac{1}{1-z}\right)^{n-k},$$

is then given by

$$a_k^{(n)} = \sum_{s=0}^{k} a_{k-s}^{(k)}\binom{s+n-k-1}{s} = \sum_{j=0}^{k} a_j^{(k)}\binom{n-j-1}{k-j}.$$

This ends the proof. □

Example. Clearly, $a_0^{(n)} = 1$ and $a_1^{(n)} = n-1$. By Theorem 9.4:

- $k = 2$: For $n \geq 3$ we have

$$a_2^{(n)} = \binom{n-1}{2}a_0^{(2)} + \binom{n-2}{1}a_1^{(2)} + \binom{n-3}{0}a_2^{(2)}\frac{(n-2)(n+1)}{2};$$

- $k = 3$: For $n \geq 4$ we have

$$\begin{aligned} a_3^{(n)} &= \binom{n-1}{3}a_0^{(3)} + \binom{n-2}{2}a_1^{(3)} + \binom{n-3}{1}a_2^{(3)} + \binom{n-4}{0}a_3^{(3)} \\ &= \frac{n(n^2-7)}{6}; \end{aligned}$$

- $k = 4$: For $n \geq 5$ we have

$$a_4^{(n)} = \binom{n-1}{4} a_0^{(4)} + \binom{n-2}{3} a_1^{(4)} + \binom{n-3}{2} a_2^{(4)} + \binom{n-4}{1} a_3^{(4)} + \binom{n-5}{0} a_4^{(4)} = \frac{n(n+1)(n^2+n-14)}{24};$$

- $k = 5$: For $n \geq 6$ we have

$$\begin{aligned} a_5^{(n)} &= \binom{n-1}{5} a_0^{(5)} + \binom{n-2}{4} a_1^{(5)} + \binom{n-3}{3} a_2^{(5)} + \\ &+ \binom{n-4}{2} a_3^{(5)} + \binom{n-5}{1} a_4^{(5)} + \binom{n-6}{0} a_5^{(5)} \\ &= \frac{1}{120}(n-1)(n+6)(n^3-9n-20); \end{aligned}$$

- $k = 6$: For $n \geq 7$ we have

$$a_6^{(n)} = \frac{1}{720} n \left(n^5 + 9n^4 - 5n^3 - 165n^2 - 356n + 516 \right).$$

For $n = 10$, $a_5^{(10)} = 1068$ and $a_6^{(10)} = 2298$, confirming the values of Q_{10}.

The coefficients of Q_n can also be obtained recursively, using

$$Q_n(z) = Q_{n-1}(z) \left(z^{n-1} + \cdots + z + 1 \right). \tag{9.18}$$

Using the coefficients of Q_n and Q_{n-1}, one obtains

$$Q_n(z) = \sum_{j=0}^{\frac{(n-1)n}{2}} a_j^{(n)} z^j = \left(\sum_{j=0}^{\frac{(n-2)(n-1)}{2}} a_j^{(n-1)} z^j \right) \left(z^{n-1} + \cdots + z + 1 \right). \tag{9.19}$$

This naturally leads to the next result.

Proposition 9.1. *The following formula holds:*

$$a_j^{(n)} = \begin{cases} a_j^{(n-1)} + \cdots + a_0^{(n-1)} & \text{if } j \in \{0, \ldots, n-1\}, \\ a_j^{(n-1)} + \cdots + a_{j-(n-1)}^{(n-1)} & \text{if } j \in \left\{ n, \ldots, \frac{n(n-1)}{2} \right\}. \end{cases} \tag{9.20}$$

A polynomial is called Λ-polynomial, if it is both palindromic and unimodal with nonnegative coefficients. It is known that the product of two or more Λ-polynomials is also a Λ-polynomial [11]. Since Q_n is a product of the Λ-polynomials $z+1, z^2+z+1, \ldots, z^{n-1}+\cdots+z+1$, it follows that Q_n is a Λ-polynomial. This property can be seen in Table 9.1. A direct proof of the unimodality of Q_n was given in [18, Proposition 2.2].

By the definition of Q_n, we obtain another interpretation of the coefficients of polynomial P_n, in terms of Kandall-Mann numbers. Indeed, from

$$P_n(z)=\left[z^n-\binom{n}{1}z^{n-1}+\binom{n}{2}z^{n-2}-\cdots+(-1)^n\binom{n}{n}\right]\left(\sum_{j=0}^{\frac{(n-1)n}{2}}a_j^{(n)}z^j\right),$$

one obtains a link between the coefficients of the polynomial P_n and Q_n.

Theorem 9.5. *The following formula holds*

$$c_j^{(n)}=\begin{cases}(-1)^n\left(a_j^{(n)}-a_{j-1}^{(n)}\binom{n}{1}+\cdots+(-1)^j a_0^{(n)}\binom{n}{j}\right) & j\in\{0,\ldots,n-1\},\\ (-1)^n\left(a_j^{(n)}-a_{j-1}^{(n)}\binom{n}{1}+\cdots+(-1)^n a_{j-n}^{(n)}\binom{n}{n}\right) & j\in\left\{n,\ldots,\frac{n(n-1)}{2}\right\}.\end{cases}$$

Example 9.1. *Using Theorem 9.5 for $j=1,\ldots,5$ and $n\geq j+1$ we obtain*
$c_0^{(n)}=(-1)^n$,
$c_1^{(n)}=(-1)^n(a_1^{(n)}-a_0^{(n)}\binom{n}{1})=(-1)^n((n-1)-n)=(-1)^{n+1}$,
$c_2^{(n)}=(-1)^n(a_2^{(n)}-a_1^{(n)}\binom{n}{1}+a_0^{(n)}\binom{n}{2})=(-1)^{n+1}$,
$c_3^{(n)}=(-1)^n(a_3^{(n)}-a_2^{(n)}\binom{n}{1}+a_1^{(n)}\binom{n}{2}-a_0^{(n)}\binom{n}{3})=0$,
$c_4^{(n)}=(-1)^n(a_4^{(n)}-a_3^{(n)}\binom{n}{1}+a_2^{(n)}\binom{n}{2}-a_1^{(n)}\binom{n}{3}+a_0^{(n)}\binom{n}{4})=0$,
$c_5^{(n)}=(-1)^n(a_5^{(n)}-a_4^{(n)}\binom{n}{1}+a_3^{(n)}\binom{n}{2}-a_2^{(n)}\binom{n}{3}+a_1^{(n)}\binom{n}{4}-a_0^{(n)}\binom{n}{5})=(-1)^n$.

9.2.6 *Some related integer sequences*

Here we examine some integer sequences related to the coefficients of the polynomials P_n and Q_n. We also conjecture that every integer n can be a coefficient of some polynomial P_m (property known to hold for cyclotomic polynomials [246]), the result being confirmed numerically for the first 10^5 numbers. We also present some some new integer sequences: A301703, A301704, and A301705, recently added by the authors to the OEIS.

9.2.6.1 The number of distinct roots of P_n

The number of distinct roots of P_n is given by

$$A(n)=\varphi(1)+\varphi(2)+\cdots+\varphi(n). \tag{9.21}$$

Indeed, by (9.6) one has $P_{n+1}(z)=P_n(z)(z^{n+1}-1)$. The new roots added by $z^{n+1}-1$ to the set of roots of P_n, are those given by the primitive roots of order $n+1$, whose number is $\varphi(n+1)$. The result follows by induction.

The sequence $A(n)$ is indexed as A002088 in the OEIS, starting with:

$$1,2,4,6,10,12,18,22,28,32,42,46,58,64,72,80,96,102,120,128,140,\ldots.$$

The asymptotic formula for $A(n)$ is given in [42, Theorem 3.7, page 72]:

$$A(n) \sim \frac{3n^2}{\pi^2} + O(n\log n).$$

Proposition 9.2. *Let $1 \leq k \leq n$ be an integer. If $z_{p,k} = e^{2\pi i \frac{p}{k}}$ is a k-th primitive root, then the multiplicity of root $z_{p,k}$ in the polynomial P_n is $\left\lfloor \frac{n}{k} \right\rfloor$. Consequently, one recovers the identity*

$$\sum_{k=1}^{n} \varphi(k) \left\lfloor \frac{n}{k} \right\rfloor = \frac{n(n+1)}{2}.$$

Proof. The root $z_{p,k}$ appears for the first time in polynomial P_k from the factor $z^k - 1$. Each of the $\varphi(k)$ roots appears as a non-primitive root of every multiple of k smaller than n.

9.2.6.2 The middle coefficients of P_n and Q_n

Formula (9.10) gives information into the sequence of middle terms. Denote by $m = \left\lfloor \frac{n(n+1)}{4} \right\rfloor$.

- If $n = 4k$, then for $m = \frac{n(n+1)}{4}$ we have $\cos\left(\frac{n(n+1)-4m}{2}t\right) = 1$ and

$$c_m^{(n)} = \frac{2^n}{\pi} \int_0^{\pi} \sin t \sin 2t \cdots \sin nt \, \mathrm{d}t. \tag{9.22}$$

  This sequence recovers A269298 in OEIS, having the starting values

$$2,2,4,6,8,16,28,50,100,196,388,786,1600,3280,6780,14060,29280,\ldots.$$

- If $n = 4k+1$, then $n(n+1) - 4m = 2$ and $\sin\left(\frac{n(n+1)-4m}{2}t\right) = \sin t$, hence

$$c_m^{(n)} = -\frac{2^n}{\pi} \int_0^{\pi} \sin^2 t \sin 2t \cdots \sin nt \, \mathrm{d}t = -c_{m+1}^{(n)}. \tag{9.23}$$

  The sequence of opposite terms is not currently indexed in OEIS:

$$1,1,1,1,2,2,3,4,6,10,17,28,52,94,176,339,651,1268,2505,4965,9916,\ldots.$$

- If $n = 4k+2$, then $n(n+1) - 4m = 2$ and $\cos\left(\frac{n(n+1)-4m}{2}t\right) = \cos t$, hence

$$c_m^{(n)} = -\frac{2^n}{\pi}\int_0^\pi \cos t \sin t \sin 2t \cdots \sin nt \, \mathrm{d}t = c_{m+1}^{(n)}. \tag{9.24}$$

The sequence of opposite terms is not currently indexed in OEIS:

$$1,1,2,3,5,10,19,34,68,135,269,544,1111,2274,4694,9729,20237,\ldots.$$

- For $n = 4k+3$, we have $m = \frac{n(n+1)}{4}$, so $\sin\left(\frac{n(n+1)-4m}{2}t\right) = 0$ and $c_m^{(n)} = 0$.

Conjecture 1. *Let n be an integer and $m = \lfloor \frac{n(n+1)}{4} \rfloor$. The middle coefficient $c_m^{(n)}$ is*

- *positive for $n = 4k$ (mentioned in A231599, without a proof);*
- *negative for $n = 4k+1$ and $n = 4k+2$.*

The sequence of middle coefficients of Q_n gives the Kendall-Mann numbers A000140 in OEIS, representing the number of permutations of the set $\{1,\ldots,n\}$ having the maximum number of inversions. The first terms are:

$$1,1,2,6,22,101,573,3836,29228,250749,2409581,25598186,296643390,\ldots.$$

The asymptotic behavior of this sequence was conjectured in A000140.

Conjecture 2. *Let n be an integer and $m = \left\lfloor \frac{n(n-1)}{4} \right\rfloor$. Then the sequence of middle coefficients $a_m^{(n)}$ of Q_n satisfies the asymptotic formula*

$$a_m^{(n)} \sim \frac{6n^{n-1}}{e^n}.$$

We are not aware of the existence of any proof at the moment.

9.2.6.3 First occurrence of n as a coefficient of a polygonal polynomial

In [246], Suzuki proved that every integer n is a coefficient for some cyclotomic polynomial. We conjecture a similar result for polygonal polynomials.

Conjecture 3. *Every integer n is a coefficient of some polygonal polynomial.*

Notice that 1 is a coefficient of P_1, while 2 first appears as a coefficient in P_4. For an integer $n \geq 0$, the sequence $a(n)$ defined by the smallest number m for which n is a coefficient of P_m produces sequence A301701, recently added by the authors to OEIS.

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	…
$a(n)$	3	1	4	10	12	17	16	19	20	22	22	23	24	25	25	25	24	26	26	28	…

The conjecture was recently checked for the first 10^5 integers.

9.2.6.4 Number of non-zero terms of P_n

The sequence of non-zero coefficients of P_n is indexed as A086781 in OEIS and starts with the terms

$$1,2,4,6,7,12,14,18,25,32,36,42,53,68,64,84,97,108,126,146,161,170,\ldots.$$

Recently, we have added the sequences below to the OEIS.

- A301703, representing the number of positive coefficients of P_n:

  $$1,2,3,3,6,6,9,13,16,18,21,27,34,32,42,47,54,62,73,79,85,96,104,113,\ldots.$$

- A301704, representing the number of negative coefficients of P_n:

  $$1,2,3,4,6,8,9,12,16,18,21,26,34,32,42,50,54,64,73,82,85,96,104,116,\ldots.$$

- A301705, representing the number of zero coefficients of P_n:

  $$0,0,1,4,4,8,11,12,14,20,25,26,24,42,37,40,46,46,45,50,62,62,69,72,\ldots.$$

9.3 Extended cyclotomic polynomials

Let $z_k = \zeta_k$, $k = 1,\ldots,\varphi(n)$, be the n-th primitive roots of unity. These can also be indexed as powers of the first primitive root $\zeta_1 = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$, i.e., ζ_1^j, with $1 \le j \le n-1$ and $\gcd(j,n) = 1$.

The **extended cyclotomic** polynomial of degree $m_1 + \cdots + m_{\varphi(n)}$ is

$$\Phi_{m_1,\ldots,m_{\varphi(n)}}(z) = \prod_{k=1}^{\varphi(n)} (z^{m_k} - \zeta_k) = \prod_{\substack{1\le j\le n-1\\ \gcd(j,n)=1}} (z^{\widetilde{m}_j} - \zeta_1^j), \tag{9.25}$$

where for $k = 1,\ldots,\varphi(n)$, we have $m_k = \widetilde{m}_j$, with j being the k-th positive integer relatively prime with n, with $1 \le j \le n-1$.

The coefficients of $\Phi_{m_1,\ldots,m_{\varphi(n)}}$, are generally complex. For example, for $n = 3$, $\zeta = \cos\frac{2\pi}{3} + i\sin\frac{2\pi}{3}$, $m_1 = 2$ and $m_2 = 3$, we obtain the polynomial

$$\Phi_{2,3}(z) = (z^2 - \zeta)(z^3 - \zeta^2) = z^5 - \zeta z^3 - \zeta^2 z^2 + 1.$$

9.3.1 Basic properties

For $m_1 = \cdots = m_{\varphi(n)} = 1$ we obtain the classical cyclotomic polynomials defined in (8.11), i.e., we have $\Phi_{1,\ldots,1} = \Phi_n$. It is well known that the coefficients $c_j^{(n)}$, $j = 0, \ldots, \varphi(n)$, of Φ_n are integers, while the cyclotomic polynomials are irreducible over $\mathbb{Z}$ (see for example, [146], Theorem 1, p. 195).

The characterization of extended cyclotomic polynomials with integer coefficients can be done by using Kronecker's Theorem (see, e.g., [75] and [123]). Here we present an alternative proof based on Galois theory.

Consider the extension $K = \mathbb{Q}(\zeta_n)/\mathbb{Q}$. This is Galois and the ring of integers of K is $O(K) = \mathbb{Z}[\zeta_n]$; see, e.g., [168, Theorem 4, Chapter IV]. By the fundamental theorem of Galois theory, an element α in K is rational if and only if $\sigma(\alpha) = \alpha$ for all σ in $Gal(K/\mathbb{Q})$ and, since for any number field K one has $O(K) \cap \mathbb{Q} = \mathbb{Z}$, we deduce that an element β in $O(K)$ is an integer if and only if $\sigma(\beta) = \beta$ for all σ in $Gal(K/\mathbb{Q})$ (see [96, Theorem 7.3.1]).

Denoting for simplicity $P = \Phi_{m_1,\ldots,m_{\varphi(n)}}$, this polynomial has coefficients in $O(K)$ and by the previous observations, these coefficients are integers precisely when $\sigma(P(z)) = P(z)$ for all $\sigma \in Gal(K/\mathbb{Q})$. To finish off, we note that $Gal(K/\mathbb{Q})$ acts transitively on the group of n-th roots of unity, and hence, for any $i, j \in (\mathbb{Z}/n\mathbb{Z})^*$, there is a σ in $Gal(K/\mathbb{Q})$ such that $\sigma(\zeta_n^i) = \zeta_n^j$. This shows that $m_i = m_j$ (the equality of $P(z)$ and $\sigma(P(z))$ is one of polynomials in $K[z]$, which is a UFD and all the factors are irreducible) and since i and j were arbitrary, it shows that $m_1 = \cdots = m_{\varphi(n)} = s$. In this case we have $\Phi_{m_1,\ldots,m_{\varphi(n)}}(z) = \Phi_n(z^s)$, where s is an arbitrary positive integer. The polynomials $\Phi_n(z^s)$ play an important role in the study of cyclotomic partitions.

9.3.2 Integral formulae for the coefficients

Here we also index powers by the primitive roots, i.e., m_k with $k \leq n-1$ and $\gcd(k,n) = 1$. In this case, for each $t \in [0, \pi]$ formula (9.2) becomes

$$\begin{aligned}\Lambda(t; m_1, \ldots, m_{\varphi(n)}; \zeta_1, \ldots, \zeta_{\varphi(n)}) &= \Lambda(t; m_1, \ldots, m_{\varphi(n)}) \\ &= \prod_{\substack{1 \leq k \leq n-1 \\ \gcd(k,n)=1}} \sin\left(m_k t - \frac{k\pi}{n}\right).\end{aligned}$$

As shown in [20, Lemma 2.1], in this case we have

$$\alpha = \sum_{\substack{1 \leq k \leq n-1 \\ \gcd(k,n)=1}} \frac{2k\pi}{n} = \varphi(n)\pi.$$

As $\varphi(n)$ is even for $n \geq 3$, using $e^{ik\pi} = (-1)^k$, $k \in \mathbb{Z}$ and Theorem 9.1 (1) the coefficients of the polynomial $\Phi_{m_1,\ldots,m_{\varphi(n)}}$ are given by

$$\begin{aligned} C_j &= \frac{(-1)^{\frac{\varphi(n)}{2}} 2^{\varphi(n)}}{\pi} \int_0^{\pi} \Lambda(t; m_1, \ldots, m_{\varphi(n)}) e^{i\left((m-2j)t + \frac{\varphi(n)}{2}\pi\right)} \, \mathrm{d}t \\ &= \frac{2^{\varphi(n)}}{\pi} \int_0^{\pi} \Lambda(t; m_1, \ldots, m_{\varphi(n)}) e^{i(m-2j)t} \, \mathrm{d}t. \end{aligned} \tag{9.26}$$

If the coefficient C_j is a real number, then by Theorem 9.1 (2), we have

$$C_j = \frac{2^{\varphi(n)}}{\pi} \int_0^{\pi} \Lambda(t; m_1, \ldots, m_{\varphi(n)}) \cos(m-2j)t \, \mathrm{d}t. \tag{9.27}$$

As a consequence, since $\cos(m-2j)t = \cos(m-2(m-j))t$, $t \in [0, 2\pi]$, from (9.27) we obtain $C_j = C_{m-j}$, $j = 0, \ldots, m$, hence we get the following result:

Corollary 9.3. *If $\Phi_{m_1,\ldots,m_{\varphi(n)}}$ has real coefficients, then it is reciprocal.*

Notice that for $m_1 = \cdots = m_{\varphi(n)}$ one recovers Theorem 8.11.

9.3.3 Some related integer sequences

The numerical calculations producing the sequences in Tables 9.3 have been computed in Matlab® and Wolfram Alpha. Some new integer sequences, not currently indexed in OEIS [211] are obtained.

Considering $m_k = 1$ for $k = 1, \ldots, \varphi(n)$, we obtain the classical cyclotomic polynomial $\Phi_{1,\ldots,1} = \Phi_n$. The coefficients of Φ_n are integers and they have been studied in detail by numerous authors. Some interesting integer sequences generated by the extended cyclotomic polynomials are defined by the number of non-zero coefficients.

Setting $n = 5$ we have $\varphi(5) = 4$ and $\zeta = \cos\frac{2\pi}{5} + i\sin\frac{2\pi}{5}$, hence

$$\Phi_{1,1,1,1}(z) = \Phi_4(z) = (z-\zeta)(z-\zeta^2)(z-\zeta^3)(z-\zeta^4) = z^4 + z^3 + z^2 + z + 1.$$

Also, setting $m_1 = 1$ and $m_k = 2$ for $k \geq 2$, for $n = 5$ we obtain

$$\begin{aligned} \Phi_{1,2,2,2}(z) = (z-\zeta)(z^2-\zeta^2)(z^2-\zeta^3)(z^2-\zeta^4) &= z^7 - \zeta z^6 - (\zeta^2 + \zeta^3 + \zeta^4)z^5 \\ &+ (1 + \zeta^3 + \zeta^4)z^4 + (1 + \zeta + \zeta^2)z^3 - (\zeta + \zeta^2 + \zeta^3)z^2 - \zeta^4 z + 1. \end{aligned}$$

When $n = 6$, $\varphi(6) = 2$, $\zeta = \cos\frac{2\pi}{6} + i\sin\frac{2\pi}{6}$ for $m_1 = 1$, $m_2 = 2$ we get

$$\Phi_{1,2}(z) = (z-\zeta)(z^2-\zeta^5) = z^3 - \zeta z^2 - \zeta^5 z + 1.$$

For $m_1 = 1$, $m_2 = 5$, where $\Phi_{1,5}(z) = (z-\zeta)(z^5-\zeta^5) = z^6 - \zeta z^5 - \zeta^5 z + 1$.

The first row of Table 9.3 recovers the sequence of non-zero coefficients of cyclotomic polynomials, indexed as A051664 in OEIS. The second row recovers the sequence A140434, counting the number of new visible points created at each step in an $n \times n$ grid ($n \geq 2$). Notice that the results in the last two rows are similar whenever n is a prime, while both sequences are not currently indexed. The n-th prime number was denoted by p_n.

Polynomial	Sequence of non-zero coefficients	OEIS
$\Phi_{1,\ldots,1}$	2, 2, 3, 2, 5, 3, 7, 2, 3, 5, 11, 3, 13, 7, 7, 2, 17, ...	A051664
$\Phi_{1,2,\ldots,2}$	2, 2, 4, 4, 8, 4, 12, 8, 12, 8, 20, 8, 24, 12, 16, 16, ...	A140434
$\Phi_{1,2,3,\ldots,3}$	2, 4, 4, 4, 10, 4, 16, 10, 16, 10, 28, 10, 34, 16, 22, ...	NEW
$\Phi_{1,2,\ldots,\varphi(n)}$	2, 2, 4, 4, 11, 4, 22, 11, 22, 11, 56, 11, 79, 22, 37, ...	NEW
$\Phi_{j_1,j_2,\ldots,j_{\varphi(n)}}$	2, 2, 4, 4, 11, 4, 22, 15, 28, 15, 56, 15, 79, 39, 61, ...	NEW

Table 9.3 The number of non-zero coefficients of the polynomial $\Phi_{m_1,\ldots,m_{\varphi(n)}}$, $n \geq 1$. The numbers $j_1 < \ldots < j_k < \ldots < j_{\varphi(n)}$ are relatively prime with n.

9.4 Extended polygonal-type polynomials

The **extended polygonal** polynomial is defined by

$$F_{m_1,\ldots,m_n}(z) = \prod_{k=1}^{n} (z^{m_k} - 1), \tag{9.28}$$

obtained for $z_1 = \cdots = z_n = 1$ in (9.1) and the integers $m_1, \ldots, m_n$.

It clearly has integer coefficients and recovers the polygonal polynomial (9.6) for $m_k = k$, $k = 1, \ldots, n$. The roots of $z^{m_k} - 1$ are the complex coordinates of the vertices of the regular m_k-gon centered at the origin, having 1 as a vertex, hence the roots of (9.28) are the complex coordinates of the vertices, with repetitions, of the regular m_k-gons with $k = 1, \ldots, n$.

9.4.1 Basic properties

According to the well-known formula $x^m - 1 = \prod_{d|m} \Phi_d(z)$, it follows that

$$F_{m_1,\ldots,m_n}(z) = \prod_{k=1}^{n} \prod_{d|m_k} \Phi_d(z),$$

i.e., the polynomial $F_{m_1,\ldots,m_n}$ has exactly $\nu(m_1) + \cdots + \nu(m_n)$ irreducible factors over $\mathbb{Z}$, where $\nu(a)$ denotes the number of divisors of a. Since all the factors are cyclotomic, $F_{m_1,\ldots,m_n}$ is a Kronecker polynomial [75].

Theorem 9.6. *The number of distinct roots of the polynomial* (9.28) *is*

$$\mathcal{R}_{m_1,\dots,m_n} = m_1 + \cdots + m_n + \sum_{j=2}^{n} (-1)^{j-1} \sum_{1 \le k_1 < \cdots < k_j \le n} gcd(m_{k_1}, \dots, m_{k_j}). \tag{9.29}$$

Proof. For $n = 2$, the polynomials $z^{m_1} - 1$ and $z^{m_2} - 1$ have m_1 and m_2 distinct roots, respectively. Out of these, a number of $\gcd(m_1, m_2)$ are common. In general, the proof follows by the inclusion-exclusion principle. Clearly, the result holds even if the numbers $m_1, \dots, m_n$ are not all distinct. □

The following formula is obtained in particular.

Remark. For $m_k = k$, $k = 1, \dots, n$, a direct counting leads to

$$\mathcal{R}_{1,\dots,n} = \sum_{k=1}^{n} \varphi(k).$$

This represents the sequence A002088 in OEIS [211], which has numerous interesting properties.

Theorem 9.7. *Let $n \ge 2$, and $m_1, \dots, m_n$ be integers and consider the set*

$$\mathcal{D}_{m_1,\dots,m_n} = \{d \in \mathbb{N} : d \text{ is a divisor of } m_k, \text{ for some } k = 1, \dots, n\}.$$

For each $d \in \mathcal{D}_{m_1,\dots,m_n}$ we denote the number of multiples of d in $\mathcal{D}_{m_1,\dots,m_n}$ by $M_d(\mathcal{D}_{m_1,\dots,m_n})$. The following identity holds:

$$\sum_{d \in \mathcal{D}_{m_1,\dots,m_n}} \varphi(d) \cdot M_d(\mathcal{D}_{m_1,\dots,m_n}) = m_1 + \cdots + m_n. \tag{9.30}$$

Proof. We count the roots of the polynomial (9.28) in two ways, considering multiplicities. A primitive root $\zeta = \cos\frac{2s\pi}{d} + i\cos\frac{2s\pi}{d}$ of order d with $\gcd(s, d) = 1$ is a root of (9.28) if and only if $d \in \mathcal{D}_{m_1,\dots,m_n}$. Indeed, for each $k = 1, \dots, n$, the roots of $z^{m_k} - 1 = 0$ are distinct, while ζ is a m_k-th root, whenever d is a divisor of m_k. Conversely, for each $d \in \mathcal{D}_{m_1,\dots,m_n}$, the number of d-th primitive roots of unity is $\varphi(d)$, while the multiplicity of each such root in (9.28) is given by $M_d(\mathcal{D}_{m_1,\dots,m_n})$. On the other hand, the polynomial (9.28) has $m_1 + \cdots + m_n$ roots, counting multiplicities. □

Corollary 9.4. *Let $1 \le k \le n$ be an integer. If $m_k = k$, $k = 1, \dots, n$, by Theorem 9.7*

$$\sum_{k=1}^{n} \varphi(k) \left\lfloor \frac{n}{k} \right\rfloor = \frac{n(n+1)}{2}.$$

In the limit cases $m_1 = \cdots = m_n$ or $n = 1$, formula (9.30) *reduces to the classical summation formula of Gauss $\sum_{d|m} \varphi(d) = m$.*

Setting $z_1 = \cdots = z_n = -1$ in formula (9.1), one obtains the **extended anti-polygonal** polynomial, given by

$$A_{m_1,\ldots,m_n}(z) = \prod_{k=1}^{n}(z^{m_k}+1). \tag{9.31}$$

Such polynomials with integer coefficients play an important role in the study of partitions. For example, the coefficient of z^m of the polynomial $A_{2m_1,\ldots,2m_n}$, where $m = m_1 + \cdots + m_n$, is the number of ordered bipartitions of the set $\{m_1,\ldots,m_n\}$ having equal sums (see, e.g., [15, 34, 40, 47]).

Clearly, the product $F_{m_1,\ldots,m_n} \cdot A_{m_1,\ldots,m_n} = F_{2m_1,\ldots,2m_n}$ is a product of exactly $\nu(2m_1) + \cdots + \nu(2m_n)$ cyclotomic polynomials. The number of irreducible factors over $\mathbb{Z}$ of the polynomial $A_{m_1,\ldots,m_n}$ is

$$\nu(2m_1) + \cdots + \nu(2m_n) - [\nu(m_1) + \cdots + \nu(m_n)]. \tag{9.32}$$

All these factors are cyclotomic, hence $A_{m_1,\ldots,m_n}$ is a Kronecker polynomial. This is a special case of Kronecker's Theorem [75, Chapter 6, pp.43-56].

9.4.2 *Coefficients of extended polygonal-type polynomials*

Notice that for the polynomial $F_{m_1,\ldots,m_n}$ given by formula (9.28), we have $z_k = 1$, hence $\alpha_k = 0$ for $k = 1,\ldots,n$, and $\alpha = \alpha_1 + \cdots + \alpha_n = 0$. We shortly denote by $\Lambda(t;m_1,\ldots,m_n)$, the function $\Lambda(t;m_1,\ldots,m_n,0,\ldots,0)$. We have

$$\Lambda(t;m_1,\ldots,m_n) = \prod_{k=1}^{n}\sin m_k t, \quad t \in [0,\pi]. \tag{9.33}$$

Since the coefficients C_j of $F_{m_1,\ldots,m_n}$ (9.28) are real, by Theorem 9.1 (2) we obtain the following result.

Theorem 9.8. *The coefficients of the polynomial $F_{m_1,\ldots,m_n}$ are given by*

$$C_j = \begin{cases} \frac{(-1)^{\frac{n}{2}}2^n}{\pi}\int_0^\pi \Lambda(t;m_1,\ldots,m_n)\cos(m-2j)t\,\mathrm{d}t & \text{if } n \text{ is even} \\ \frac{(-1)^{\frac{n+1}{2}}2^n}{\pi}\int_0^\pi \Lambda(t;m_1,\ldots,m_n)\sin(m-2j)t\,\mathrm{d}t & \text{if } n \text{ is odd.} \end{cases} \tag{9.34}$$

For the polynomial $A_{m_1,\ldots,m_n}$ (9.31) one has $z_k = -1$, hence $\alpha_k = \pi$ for $k = 1,\ldots,n$ and $\alpha = \alpha_1 + \cdots + \alpha_n = n\pi$. We denote $\Lambda(t;m_1,\ldots,m_n,\pi,\ldots,\pi)$ by $\widetilde{\Lambda}(t;m_1,\ldots,m_n)$, and obtain

$$\widetilde{\Lambda}(t;m_1,\ldots,m_n) = \prod_{k=1}^{n}\cos m_k t, \quad t \in [0,\pi]. \tag{9.35}$$

The following result can be obtained from Theorem 9.1 (2).

Theorem 9.9. *The coefficients of the polynomial $A_{m_1,\ldots,m_n}$ are given by*

$$C_j = \frac{2^n}{\pi}\int_0^{\pi} \widetilde{\Lambda}(t;m_1,\ldots,m_n)\cos(m-2j)t\,\mathrm{d}t, \quad j=0,\ldots,m. \tag{9.36}$$

It also follows that

$$\int_0^{\pi} \widetilde{\Lambda}(t;m_1,\ldots,m_n)\sin(m-2j)t\,\mathrm{d}t = 0, \quad j=0,\ldots,m.$$

Remark. An interesting particular case is obtained for $m_k = k$, $k = 1,\ldots,n$. If $S(n)$ is the number of ordered bipartitions of $\{1,2,\ldots,n\}$ into sets having equal sums, then this is the middle coefficient of the polynomial $A_{1,2,\ldots,n}$, that is the coefficient of $z^{\frac{n(n+1)}{2}}$ when $n \equiv 0$ or $n \equiv 3 \pmod 4$.

In [40], D. Andrica and I. Tomescu conjectured the asymptotic formula

$$S(n) \sim \sqrt{\frac{6}{\pi}} \cdot \frac{2^n}{n\sqrt{n}},$$

where $f(n) \sim g(n)$ means that $\lim\limits_{n\to\infty} f(n)/g(n) = 1$. This formula has been proven by B. D. Sullivan [245], using the corresponding integral formula from Theorem 9.9 and complicated analytic techniques.

9.4.3 Some related integer sequences

The extended polygonal polynomial $F_{m_1,\ldots,m_n}$ has integer coefficients. For example, when $n = 4$ and $m_1 = 1$, $m_2 = 2$, $m_3 = 3$ and $m_4 = 4$ one has

$$\begin{aligned} F_{1,2,3,4}(z) &= (z-1)(z^2-1)(z^3-1)(z^4-1) \\ &= z^{10} - z^9 - z^8 + 2z^5 - z^2 - z + 1, \end{aligned}$$

which has 7 non-zero coefficients of which the highest is equal to 2.

In this section we explore some integer sequences related to the number of non-zero, and the maximum coefficients of the polynomial $F_{m_1,\ldots,m_n}$, the for the sequence $F_{m_1,\ldots,m_n}$, as well as to the number of irreducible factors over integers for the polynomial $A_{m_1,\ldots,m_n}$. The numerical calculations producing the sequences presented in the Tables 9.3-9.7 in this section, have been computed in Matlab® and Wolfram Alpha. In this process we recover some new integer sequences, not currently indexed in OEIS [211].

9.4.3.1 The number of non-zero coefficients of $F_{m_1,\ldots,m_n}$

The sequence giving the number of non-zero coefficients of $F_{m_1,\ldots,m_n}$ $(n \geq 1)$ recovers some known integer sequences, as well as a novel sequence when $m_n = p_n$ is the n-th prime $(n \geq 1)$, as seen in Table 9.4. The first and third lines are identical, since $F_{km_1,\ldots,km_n}(z) = F_{m_1,\ldots,m_n}(z^k)$, for all $k \in \mathbb{N}$.

Polynomial	Sequence of non-zero coefficients	OEIS
$F_{1,\ldots,n}$	2, 4, 6, 7, 12, 14, 18, 25, 32, 36, 42, 53, 68, 64, 84, ...	A086781
$F_{1,\ldots,2n-1}$	2, 4, 8, 15, 24, 35, 48, 63, 80, 99, 120, 143, 168, 195, ...	A082562
$F_{2,\ldots,2n}$	2, 4, 6, 7, 12, 14, 18, 25, 32, 36, 42, 53, 68, 64, 84, ...	A086781
$F_{1,\ldots,n^2}$	2, 4, 8, 16, 24, 40, 68, 103, 162, 236, 344, 453, 612, ...	A225549
$F_{p_1,\ldots,p_n}$	2, 4, 6, 8, 14, 20, 24, 32, 46, 66, 92, 138, 162, 204, ...	NEW

Table 9.4 The number of non-zero coefficients of the polynomial $F_{m_1,\ldots,m_n}$, $n \geq 1$.

9.4.3.2 The maximum coefficient of $F_{m_1,\ldots,m_n}$

The maximum coefficient of $F_{m_1,\ldots,m_n}$ $(n \geq 1)$ recovers some known integer sequences when $m_n = n$ or $m_n = 2n$, while it also generates some novel sequences in the other cases, as seen in Table 9.5.

Polynomial	Sequence of maximum coefficients of $F_{m_1,\ldots,m_n}$	OEIS
$F_{1,\ldots,n}$	1, 1, 1, 2, 1, 2, 2, 2, 2, 3, 2, 4, 3,3, 4, 6, 5, 6, 7, 8, ...	A086376
$F_{1,\ldots,2n-1}$	1, 1, 1, 2, 2, 3, 5, 8, 13, 22, 38, 68, 118, 211, 380, ...	NEW
$F_{2,\ldots,2n}$	1, 1, 1, 2, 1, 2, 2, 2, 2, 2, 3, 2, 4, 3, 3, 4, 6, 5, 6, 7, 8, ...	A086376
$F_{1,\ldots,n^2}$	1, 1, 1, 1, 1, 1, 2, 2, 3, 3, 4, 6, 7, 8, 11, 14, 12, 12, ...	NEW
$F_{p_1,\ldots,p_n}$	1, 1, 1, 1, 1, 1, 1, 1, 1, 2, 2, 2, 3, 4, 6, 8, 12, 17, 30,...	NEW

Table 9.5 The maximum coefficient of the polynomial $F_{m_1,\ldots,m_n}$, $n \geq 1$.

9.4.3.3 The number of irreducible factors over integers of $A_{m_1,\ldots,m_n}$

The number of irreducible factors of $A_{m_1,\ldots,m_n}$ given by (9.32), simplifies to $\sum_{k=1}^{n} \frac{\nu(m_k)}{\alpha_k+1}$, where $m_k = 2^{\alpha_k} m'_k$, with m'_k odd, $k = 1,\ldots,n$. Some sequences arise naturally for particular choices of m_k, $k = 1,\ldots,n$.

The interpretations known for the OEIS sequence A001227 in the first row of Table 9.6 include: the number of odd divisors of n, the number of ways to write n as difference of two triangular numbers, the number of partitions of n into consecutive positive integers, or the number of factors in the factorization of the n-th Chebyshev polynomial of the first kind.

Polynomial	Number of irreducible factors	OEIS
z^n+1	1, 1, 2, 1, 2, 2, 2, 1, 3, 2, 2, 2, 2, 2, 4, ...	A001227
$z^{3n}+1$	2, 2, 3, 2, 4, 3, 4, 2, 4, 4, 4, 3, 4, 4, 6, ...	NEW
$z^{9n}+1$	3, 3, 4, 3, 6, 4, 6, 3, 5, 6, 6, 4, 6, 6, 8, ...	NEW

Table 9.6 Number of irreducible factors over the integers of the polynomial $z^{m_n}+1$, for $m_n=n$, $m_n=3n$ and $m_n=9n$, $n\geq 1$.

Polynomial	Number of irreducible factors of $A_{m_1,\ldots,m_n}$	OEIS
$A_{1,\ldots,n}$	1, 2, 4, 5, 7, 9, 11, 12, 15, 17, 19, 21, 23, 25, 29, ...	A060831
$A_{3,\ldots,3n}$	2, 4, 7, 9, 13, 16, 20, 22, 26, 30, 34, 37, 41, 45, 51, ...	NEW
$A_{9,\ldots,9n}$	3, 6, 10, 13, 19, 23, 29, 32, 37, 43, 49, 53, 59, 65, 73, ...	NEW

Table 9.7 The number of irreducible factors over the integers of the polynomial $A_{m_1,\ldots,m_n}$, for $m_n=n$, $m_n=3n$ and $m_n=9n$, $n\geq 1$.

Some interpretations known for the OEIS sequence A060831 in the first row of Table 9.7 are the following: the number of odd divisors present in $\{1,\ldots,n\}$, the number of sums less than or equal to n of sequences of consecutive positive integers, or the total number of partitions of all positive integers less or equal to n into an odd number of equal parts. The asymptotic formula for the OEIS sequence A060831 was conjectured in 2019 as $a(n)\sim n\left(\log(2n)+2\gamma-1\right)/2$, where γ is the Euler-Mascheroni constant.

9.5 Gaussian, multinomial and Catalan polynomials

In what follows we shall present some properties of the Gaussian, multinomial and Catalan polynomials and some integral formulae for their coefficients, based on the papers [18] and [19].

9.5.1 Coefficients of Gaussian polynomials

Let m and r be positive integers. The **Gaussian polynomial** is defined by

$$\binom{m}{r}_z=\sum_{k=0}^{r(m-r)}C_j^{(m,r)}z^j=\frac{P_m(z)}{P_r(z)P_{m-r}(z)}=\begin{cases}\frac{(z^{m-r+1}-1)\cdots(z^m-1)}{(z-1)\cdots(z^r-1)} & \text{if } r\leq m\\ 0 & \text{if } r>m.\end{cases}\tag{9.37}$$

Notice that while formula (9.37) seems to involve a rational function, the division is actually exact in the ring $\mathbb{Z}[z]$, of polynomials with integer coefficients, and it generates a polynomial of degree $r(m-r)$.

The Gaussian polynomial (9.37) has distinct roots roots (see. e.g., Chen and Hou [88]), while its factorization in terms of cyclotomic polynomials was given by Knuth and Wilf [162] as

$$\binom{m}{r}_z = \prod_{k=1}^{m} [\Phi_k(z)]^{\lfloor m/k \rfloor - \lfloor r/k \rfloor - \lfloor (m-r)/k \rfloor}, \tag{9.38}$$

where $\Phi_k(z)$ denotes the k-th cyclotomic polynomial.

The coefficients $C_j^{(m,r)}$, $j = 0, \ldots, r(m-r)$, have many interesting properties and interpretations. The coefficient $C_j^{(m,r)}$ represents the number of partitions of number j whose Ferrers diagram fits into a $r \times (m-r)$ rectangle. Also, if $\delta = \delta_1 \delta_2 \cdots \delta_r$ is a r-subset of $[n]$, and $\sigma(\delta) = \sum_{i=1}^{r} \delta_i$ (weight of δ), then $C_j^{(m,r)}$ is the number of r-subsets of $[n]$ with weight $j + \frac{r(r+1)}{2}$ [212].

It is known that the sequence $C_j^{(m,r)}$, $j = 0, \ldots, r(m-r)$, is unimodal. First stated by Cayley in 1856, this property was proved by Sylvester in 1878, and a constructive proof was first given by O'Hara in 1990 [212]. However, this sequence is not always log-concave (see, e.g., $\binom{4}{2}_z = 1 + z + 2z^2 + z^3 + z^4$), as shown by Stanley in 1989 [244]. Other generalized Gaussian coefficients were proved to be unimodal by Kirillov in 1992 [157].

By simple work with complex numbers [6], and using formula

$$z^k - 1 = (\cos 2kt - 1) + i \sin 2kt = 2ie^{ikt} \sin kt, \tag{9.39}$$

from Theorem 9.1 (2) applied for the function

$$\Lambda_r^m(t) = \prod_{k=1}^{r} \frac{\sin(m-r+k)t}{\sin kt}, \tag{9.40}$$

we obtain a formula for the coefficients of the Gaussian polynomial $\binom{m}{r}_z$.

Theorem 9.10. *The coefficients of the polynomial $\binom{m}{r}_z$ are given by*

$$C_j^{(m,r)} = \frac{1}{\pi} \int_0^{\pi} \Lambda_r^m(t) \cdot \cos[r(m-r) - 2j]\, t \, \mathrm{d}t, \quad j = 0, \ldots, r(m-r). \tag{9.41}$$

Remark. By Theorem 9.10 we can easily prove that the polynomial $\binom{m}{r}_z$ is palindromic. Indeed, for $j = 0, \ldots, r(m-r)$, one obtains

$$\begin{aligned} C_{r(m-r)-j}^{(m,r)} &= \frac{1}{\pi} \int_0^{\pi} \Lambda_r^m(t) \cdot \cos[r(m-r) - 2(r(m-r) - j)]\, t \, \mathrm{d}t \\ &= \frac{1}{\pi} \int_0^{\pi} \Lambda_r^m(t) \cdot \cos[-r(m-r) + 2j]\, t \, \mathrm{d}t = C_j^{(m,r)}. \end{aligned} \tag{9.42}$$

A simple formula for the middle coefficients can also be derived.

Proposition 9.3. *The middle coefficient of the polynomial* $\binom{m}{r}_z$ *is given by:*
1. If $r(m-r) = 2k$, *then*

$$C_k^{(m,r)} = \frac{1}{\pi}\int_0^\pi \Lambda_k^m(t)\,\mathrm{d}t.$$

2. If $r(m-r) = 2k+1$, *then*

$$C_k^{(m,r)} = C_{k+1}^{(m,r)} = \frac{1}{\pi}\int_0^\pi \Lambda_k^m(t)\cdot\cos t\,\mathrm{d}t.$$

9.5.2 Coefficients of multinomial polynomials

Let $s, m, m_1 \ldots, m_s$ be positive integers such that $m_1 + \cdots + m_s = m$. The **multinomial polynomial** is defined by the formula:

$$\binom{m}{m_1,\cdots,m_s}_z = \frac{P_m(z)}{P_{m_1}(z)\cdots P_{m_s}(z)} = \sum_{j=0}^{M} C_j^{m_1,\cdots,m_s} z^j, \tag{9.43}$$

Clearly, for $s = 2$ and $m_1 = r$, one obtains the Gaussian polynomial. While the formula (9.43) seems to involve a rational function, the division is in fact exact in the ring $\mathbb{Z}[z]$. The degree of this polynomial is

$$\begin{aligned} M &= \frac{m(m+1)}{2} - \sum_{j=1}^{s}\frac{m_j(m_j+1)}{2} \\ &= \frac{1}{2}\left[m^2 - (m_1^2 + m_2^2 + \cdots + m_s^2)\right] \\ &= \sum_{1\le k<l\le s} m_k m_l. \end{aligned} \tag{9.44}$$

The multinomial polynomial can be factorized in irreducible factors involving the cyclotomic polynomials, as shown by Chen and Huo in [88, Lemma 1], and naturally extends formula (9.38).

Proposition 9.4. *The multinomial polynomial* (9.43) *can be factorized as*

$$\binom{m}{m_1,\cdots,m_s}_z = \prod_{k=1}^{m}[\Phi_k(z)]^{\lfloor m/k\rfloor - \lfloor m_1/k\rfloor - \lfloor m_2/k\rfloor - \cdots - \lfloor m_s/k\rfloor},$$

where $\Phi_k(z)$ *denotes the k-th cyclotomic polynomial.*

From this result we can obtain an interesting identity concerning the degree of this polynomial, which involves the floor function.

Theorem 9.11. *Let $m, m_1, m_2, \dots, m_s$ be positive integers which satisfy the identity $m = m_1 + m_2 + \cdots + m_s$. The following relation holds:*

$$\sum_{k=1}^{m} \varphi(k) \left(\lfloor m/k \rfloor - \lfloor m_1/k \rfloor - \lfloor m_2/k \rfloor - \cdots - \lfloor m_s/k \rfloor \right) = M. \tag{9.45}$$

By using again the result in Theorem 9.1 (2) with the function

$$\Lambda^{m}_{m_1,\dots,m_s}(t) = \frac{\prod_{k=1}^{m} \sin kt}{\prod_{j=1}^{s} \left(\prod_{k=1}^{m_j} \sin kt \right)}, \tag{9.46}$$

we get an integral formula for the coefficients of the polynomial $\binom{m}{m_1,\cdots,m_s}_z$.

Theorem 9.12. *The coefficients of the polynomial $\binom{m}{m_1,\cdots,m_s}_z$ are given by*

$$C_j^{m_1,\dots,m_s} = \frac{1}{\pi} \int_0^{\pi} \Lambda^{m}_{m_1,\dots,m_s}(t) \cdot \cos\left(M - 2j\right) t \, \mathrm{d}t, \quad j = 0, \dots, M. \tag{9.47}$$

Notice that the integral in formula (9.47) is not singular, since we have

$$\lim_{t \to 0} \Lambda^{m}_{m_1,\dots,m_s}(t) = \frac{m!}{\prod_{j=1}^{s} m_j!} = \binom{m}{m_1, \dots, m_s}.$$

Remark. Using Theorem 9.12 it follows that the polynomial $\binom{m}{m_1,\cdots,m_s}_z$ is palindromic. Indeed, for $j = 0, \dots, M$, one obtains

$$\begin{aligned} C_{M-j}^{m_1,\dots,m_s} &= \frac{1}{\pi} \int_0^{\pi} \Lambda^{m}_{m_1,\dots,m_s}(t) \cdot \cos\left(M - 2(M-j)\right) t \, \mathrm{d}t \\ &= \frac{1}{\pi} \int_0^{\pi} \Lambda^{m}_{m_1,\dots,m_s}(t) \cdot \cos\left(-M + 2j\right) t \, \mathrm{d}t = C_j^{m_1,\dots,m_s}. \end{aligned} \tag{9.48}$$

A formula for the middle coefficients can also be derived.

Proposition 9.5. *The middle coefficient of $\binom{m}{m_1,\cdots,m_s}_z$ is given by the following formulae (depending on the parity of M):*
1°. *If $M = 2k$, then*

$$C_k^{m_1,\dots,m_s} = \frac{1}{\pi} \int_0^{\pi} \Lambda^{m}_{m_1,\dots,m_s}(t) \, \mathrm{d}t. \tag{9.49}$$

2°. *If $M = 2k + 1$, then*

$$C_k^{m_1,\dots,m_s} = C_{k+1}^{m_1,\dots,m_s} = \frac{1}{\pi} \int_0^{\pi} \Lambda^{m}_{m_1,\dots,m_s}(t) \cdot \cos t \, \mathrm{d}t. \tag{9.50}$$

9.5.3 Coefficients of Catalan polynomials

For a positive integer m, the m-th **Catalan polynomial** is defined by

$$Q_m(z) = \frac{z-1}{z^{m+1}-1}\binom{2m}{m}_z = \frac{z-1}{z^{m+1}-1}\cdot\frac{P_{2m}(z)}{P_m^2(z)} = \sum_{j=0}^{m(m-1)} c_j^m z^j, \tag{9.51}$$

having degree $m(m-1)$ and at least $m-1$ irreducible factors [88].

Applying the formula (9.39), we obtain

$$\binom{2m}{m}_z = e^{im^2t}\frac{\prod_{k=1}^{2m}\sin kt}{\left(\prod_{k=1}^{m}\sin kt\right)^2}.$$

Denoting for simplicity by

$$\Psi^m(t) = \frac{\sin t}{\sin(m+1)t}\Lambda_m^{2m}(t), \quad t\in[0,\pi],$$

by Theorem 9.1 (2) we obtain the following result

Theorem 9.13. *The coefficients of the polynomial $Q_m(z)$ are given by*

$$c_j^m = \frac{1}{\pi}\int_0^\pi \Psi^m(t)\cdot\cos\left[m(m-1)-2j\right]t\,\mathrm{d}t, \quad j=0,\dots,m(m-1). \tag{9.52}$$

Notice that the integral in formula (9.52) is not singular, since we have

$$\lim_{t\to 0}\Psi^m(t) = \frac{1}{m+1}\binom{2m}{m},$$

which represents the m-th Catalan number.

Remark. Theorem 9.13 can be used to prove that the Catalan polynomial is palindromic. Indeed, for $j=0,\dots,m(m-1)$, one obtains

$$\begin{aligned} c_{m(m-1)-j}^m &= \frac{1}{\pi}\int_0^\pi \Psi^m(t)\cdot\cos\left[m(m-1)-2(m(m-1)-j)\right]t\,\mathrm{d}t \\ &= \frac{1}{\pi}\int_0^\pi \Psi^m(t)\cdot\cos\left[-m(m-1)+2j\right]t\,\mathrm{d}t = c_j^m. \end{aligned} \tag{9.53}$$

We also give an integral formula for the middle coefficient.

Proposition 9.6. *The middle coefficient of $Q_m(z)$ is given by:*

$$c_{\frac{m(m-1)}{2}}^m = \frac{1}{\pi}\int_0^\pi \Psi^m(t)\,\mathrm{d}t.$$

Chapter 10
Partitions and Recurrences

An integer partition is a way of writing an integer as a sum of natural numbers. The study of partitions was pioneered by Euler (1748), who introduced many concepts which are still in use, and proved fundamental results concerning partitions into distinct parts, or into odd parts. Since that time, numerous mathematicians including Gauss, Cauchy, Jacobi, Weierstrass, MacMahon, Hardy, Ramanujan, Erdös or Andrews contributed to the study of partitions. Key details about the history of partitions can be found in the classical books of Andrews [12] and [13], or in the review article by Pak [217], which focuses on bijective proofs of classical partitions identities.

Partitions play a significant role in many branches of mathematics, like combinatorics, group representation theory, or symmetric polynomials. Partitions have direct applications to classical combinatorial optimization problems such as the Bin Packing Problem (BPP), the Multiprocessor Scheduling Problem (MSP) and the $0-1$ Multiple Knapsack Problem (MKP) [99].

In Section 10.1 we present key results and problems concerning partitions, including the signum equation, and the Laurent ring $\mathbb{Z}[X, X^{-1}]$.

In Section 10.2 we investigate in detail the ordered 2-partitions of multisets with equal sums, which are related to the signum equation, based on the results presented in our paper [47]. We provide integral formulae for the number of such partitions, and we explore the scenario when the multiset contains $m \geq 1$ copies of the set $\{1, \ldots, n\}$. Some conjectures are stated.

In Section 10.3 we analyze the number of ordered k-partitions with equal sums of a multiset, for which we derive generating functions, integral formulae, and recurrences. Numerical experiments are used to illustrate the results and to formulate some new conjectures. The generating function approach proposed by Andrica in [14] opened the way to numerous novel results related to multi-partitions with equal sums.

Examples involving particular case of 3-partitions with equal sums are also provided [15]. Some sequences resulting from this investigation were new, or provided novel context to existing entries in OEIS.

10.1 Some classical partition problems and preliminaries

Euler showed that the number of ways in which an integer $n \geq 2$ can be partitioned as a sum of positive integers is given by the generating function

$$\sum_{n=0}^{\infty} p(n)x^n = \prod_{k=1}^{\infty} \left(\frac{1}{1-x^k} \right). \tag{10.1}$$

In fact, Euler has also considered the partition of number n obtained when the summands only belong to a certain set of integers A. More details about generating functions related to partitions can be found in [260].

A first asymptotic formula for $p(n)$ was given by Hardy and Ramanujan, who in 1918 proposed the following result

$$p(n) \sim \frac{1}{4n\sqrt{3}} \exp\left(\pi \sqrt{\frac{2n}{3}} \right), \tag{10.2}$$

valid as $n \to \infty$. An elementary proof was given in 1942 by Erdös [109].

Of particular interest are the partitions of the set $\{1,2,\ldots,n\}$, related to the signum equation, and that of k-partitions with equal sums.

10.1.1 The signum equation

The **signum equation** is classic a combinatorial problem, first considered by S. Finch [114]. For a given positive integer n, the level n solution of this equation denoted by $S(n)$, which corresponds to the number of ways of choosing $+$ and $-$ such that $\pm 1 \pm 2 \pm 3 \pm \cdots \pm n = 0$. This also represents the number of partitions of $\{1,2,\ldots,n\}$ in two sets with equal sums. The sequence $\{S(n)\}_{n\geq 0}$ is indexed as A063865 in the Online Encyclopedia of Integer Sequences (OEIS) [211], and its first few terms are

$$1,0,0,2,2,0,0,8,14,0,0,70,124,0,0,722,1314,0,0,\ldots$$

For example, $S(7) = 8$ since $1 + \cdots + 7 = 28$ and

$$14 = 1+6+7 = 2+5+7 = 3+4+7 = 3+5+6.$$

The asymptotic formula for $S(n)$ was conjectured by Andrica and Tomescu [40] in 2002:

$$\lim_{\substack{n\to\infty \\ n\equiv 0 \text{ or } 3 (mod 4)}} \frac{S(n)}{\frac{2^n}{n\sqrt{n}}} = \sqrt{\frac{6}{\pi}}.$$

The result was proved in 2013 by Sullivan [245], by analytic methods. Proof details and possible extensions, as well as connections to Erdös-Suranyi representations, were suggested in [34, 35]. More details on these sequence were provided earlier in Chapter 3.

Starting from an interesting analysis problem with trigonometric integrals [14], Andrica established a generating function which allowed novel approaches in the study of 2-partitions with equal sums for multisets. The exact value of related trigonometric integrals involving products of sine or cosine function has been studied in [73], and inspired numerous Olympiad problems as shown in [25].

For details regarding the general theory of multisets one can check the paper by Stanley [243]. The connection with unimodal polynomials is made in [41] and with some aspects in special representations of integers, known as Erdös-Suranyi representations are given in [104], [108] and [114].

10.1.2 The Laurent ring $\mathbb{Z}[X, X^{-1}]$

Recall that a Laurent polynomial with integer coefficients has the form

$$p = \sum_{k \in \mathbb{Z}} a_k X^k, \quad a_k \in \mathbb{Z},$$

where X is a formal variable, and only finitely many coefficients a_k are nonzero. Two Laurent polynomials are equal if their coefficients are equal. Such expressions can be added, multiplied, and brought back to the same form by reducing the corresponding similar terms.

Formulae for addition and multiplication are the same as for the ordinary polynomials, with the only difference being that both positive and negative powers of X can be present. The set of Laurent polynomials $\mathbb{Z}[X, X^{-1}]$ is a ring with respect to the addition and multiplication.

A Laurent polynomial $p \in \mathbb{Z}[X, X^{-1}]$ is *symmetric* if it satisfies the relation $p(X) = p(X^{-1})$. This property is equivalent to $a_{-k} = a_k$, for all $k \in \mathbb{Z}$. The maximal positive integer s with $a_s \neq 0$ defines the degree of p. The set of all symmetric Laurent polynomials $\mathbb{Z}_{\text{symm}}[X, X^{-1}]$ is a subring of $\mathbb{Z}[X, X^{-1}]$.

10.2 Ordered 2-partitions of multisets

The interplay between integer sequences and partitions has led to numerous interesting results, with implications in generating functions, integral

formulae, or combinatorics. An illustrative example is the number of solutions at level n to the signum equation. Here we present some of the results and conjectures concerning 2-partitions of multisets, given in [47].

10.2.1 Definitions and notations

Let $\alpha_1,\ldots,\alpha_n \in \mathbb{R}$ and $m_1,\ldots,m_n \in \mathbb{N}$, and consider the multiset

$$M = \{\underbrace{\alpha_1,\cdots,\alpha_1}_{m_1 \text{ times}},\ldots,\underbrace{\alpha_n,\cdots,\alpha_n}_{m_n \text{ times}}\}.$$

For $s = 1,\ldots,n$, we call m_s the **multiplicity** of element α_s in the multiset M, while $\sigma(M) = \sum_{s=1}^{n} m_s\alpha_s$ is the **sum** of the elements of M.

Definition 10.1. Let $\boldsymbol{\alpha} = (\alpha_1,\ldots,\alpha_n)$, $\mathbf{m} = (m_1,\ldots,m_n)$ and denote by $S(\mathbf{m};\boldsymbol{\alpha})$ the number of ordered 2-partitions of M having equal sums, i.e., the number of pairs (C_1,C_2) of subsets of M satisfying the properties

(i) $C_1 \cup C_2 = M$ and $C_1 \cap C_2 = \emptyset$;

(ii) $\sum\limits_{x\in C_1} x = \sum\limits_{x\in C_2} x = \frac{1}{2}\sum_{i=1}^{n} m_i\alpha_i$.

One can check that $S(\mathbf{m};\boldsymbol{\alpha})$ is the constant term in the expansion

$$F(z) = \left(z^{\alpha_1} + \frac{1}{z^{\alpha_1}}\right)^{m_1}\left(z^{\alpha_2} + \frac{1}{z^{\alpha_2}}\right)^{m_2}\cdots\left(z^{\alpha_n} + \frac{1}{z^{\alpha_n}}\right)^{m_n}. \tag{10.3}$$

Clearly, from the relation $F(z) = F(1/z)$ it follows that the expression of $F(z)$ in (10.3), after we expand, is a symmetric Laurent polynomial of variable z and degree $\sum_{i=1}^{k} m_i\alpha_i$. When $m_1 = \ldots = m_k = m$, we say that the elements of the multiset M are of the multiplicity m.

Expanding $F(z)$ one obtains its algebraic form

$$F(z) = c_0(\mathbf{m};\boldsymbol{\alpha}) + \sum_{j\in\mathbb{Z}\setminus\{0\}} c_j z^j, \tag{10.4}$$

where all coefficients c_j of F are zero, excepting a finite number. For the unity of notation, we use $c_0(\mathbf{m};\boldsymbol{\alpha}) = S(\mathbf{m};\boldsymbol{\alpha})$ and $c_j = c_j(\mathbf{m};\boldsymbol{\alpha})$, for $j \in \mathbb{Z}\setminus\{0\}$.

10.2.2 Integral formulae

Setting $z = \cos t + i\sin t$ in (10.3) and (10.4) we get

$$2^{m_1+\cdots+m_k}\prod_{s=1}^{k}(\cos\alpha_s t)^{m_s}=c_0(\mathbf{m};\boldsymbol{\alpha})+\sum_{j\in\mathbb{Z}\setminus\{0\}}c_j(\cos jt+i\sin jt).$$

Integrating in t over $[0,2\pi]$, we obtain the following formula

$$c_0(\mathbf{m};\boldsymbol{\alpha})=\frac{2^{m_1+\cdots+m_n}}{2\pi}\int_0^{2\pi}\prod_{s=1}^{n}(\cos\alpha_s t)^{m_s}dt. \tag{10.5}$$

The combinatorial intepretation of the coefficient $c_j(\mathbf{m};\boldsymbol{\alpha})$ is the number of representations of the integer j as

$$j=\underbrace{\pm\alpha_1\pm\cdots\pm\alpha_1}_{m_1\ times}\pm\cdots\pm\underbrace{\alpha_n\pm\cdots\pm\alpha_n}_{m_k\ times},$$

for all possible $2^{m_1+\cdots+m_n}$ choices of signs $+$ and $-$.

If we multiply the relation (10.4) by z^{-j} we get

$$z^{-j}F(z)=c_j(\mathbf{m};\boldsymbol{\alpha})+\sum_{l\neq j}c_l z^l, \tag{10.6}$$

hence by integrating in t over $[0,2\pi]$, we have

$$c_j(\mathbf{m};\boldsymbol{\alpha})=\frac{2^{m_1+\cdots+m_n}}{2\pi}\int_0^{2\pi}\cos jt\prod_{s=1}^{n}(\cos\alpha_s t)^{m_s}dt. \tag{10.7}$$

10.2.3 Multisets with equal multiplicity

Consider the multiset $M=[n]_m$ consisting of m copies of each element of the set $[n]=\{1,\ldots,n\}$. In the paper [47] we have studied some properties of the symmetric Laurent polynomial defined by the expansion

$$\begin{aligned}F_{n,m}(z)&=\left(z+\frac{1}{z}\right)^m\left(z^2+\frac{1}{z^2}\right)^m\cdots\left(z^n+\frac{1}{z^n}\right)^m\\&=\sum_{j\in\mathbb{Z}}c_j^{(m)}(n)z^j,\end{aligned} \tag{10.8}$$

which is a special case of the polynomial in (10.3), obtained for $k=n$ and $\alpha_1=1,\ldots,\alpha_n=n$. Notice that the symmetric Laurent polynomial $F_{n,m}(z)$ has the degree $\dfrac{mn(n+1)}{2}$.

If we multiply the polynomials $F_{n,k}(z)$ and $F_{n,l}(z)$, we have the following formula for the coefficients of $F_{n,k+l}(z)$

$$c_d^{(k+l)}(n) = \sum_{j\in\mathbb{Z}} c_{j+d}^{(k)}(n) c_j^{(l)}(n), \quad d \in \mathbb{Z}. \tag{10.9}$$

Recurrent formulae for $c_j^{(m)}(n)$ as a function of terms of the form $c_j^{(m)}(n)$, which allow an efficient numerical computation.

For $m = 1$ one obtains $c_j^{(1)}(n)$ recursively as

$$\begin{aligned} F_{n,1}(z) &= \sum_{j\in\mathbb{Z}} c_j^{(1)}(n) z^j = F_{n-1,1}(z)\left(z^n + \frac{1}{z^n}\right) \\ &= \left(\sum_{j\in\mathbb{Z}} c_j^{(1)}(n-1) z^j\right)\left(z^n + \frac{1}{z^n}\right) \\ &= \left(\sum_{j\in\mathbb{Z}} c_j^{(1)}(n-1) z^{j+n}\right) + \left(\sum_{j\in\mathbb{Z}} c_j^{(1)}(n-1) z^{j-n}\right) \\ &= \sum_{j\in\mathbb{Z}} \left(c_{j-n}^{(1)}(n-1) + c_{j+n}^{(1)}(n-1)\right) z^j. \end{aligned}$$

Hence,

$$c_j^{(1)}(n) = c_{j-n}^{(1)}(n-1) + c_{j+n}^{(1)}(n-1), \text{ for } j \in \mathbb{Z}. \tag{10.10}$$

Similarly, $c_j^{(2)}(n)$ can also be obtained recurrently by

$$\begin{aligned} F_{n,2}(z) &= \sum_{j\in\mathbb{Z}} c_j^{(2)}(n) z^j = F_{n-1,2}(z)\left(z^n + \frac{1}{z^n}\right)^2 \\ &= \left(\sum_{j\in\mathbb{Z}} c_j^{(2)}(n-1) z^j\right)\left(z^{2n} + 2 + \frac{1}{z^{2n}}\right) \\ &= \sum_{j\in\mathbb{Z}} c_j^{(2)}(n-1) z^{j+2n} + \sum_{j\in\mathbb{Z}} c_j^{(2)}(n-1) z^j + \sum_{j\in\mathbb{Z}} c_j^{(2)}(n-1) z^{j-2n} \\ &= \sum_{j\in\mathbb{Z}} \left(c_{j-2n}^{(2)}(n-1) + 2c_j^{(2)}(n-1) + c_{j+2n}^{(2)}(n-1)\right) z^j. \end{aligned}$$

Hence, for $j \in \mathbb{Z}$ one obtains

$$c_j^{(2)}(n) = c_{j-2n}^{(2)}(n-1) + 2c_j^{(2)}(n-1) + c_{j+2n}^{(2)}(n-1). \tag{10.11}$$

The following recurrences are valid for $j \in \mathbb{Z}$ and $n \geq 1$.

$$c_j^{(3)}(n) = c_{j-3n}^{(3)}(n-1) + 3c_{j-n}^{(3)}(n-1) + 3c_{j+n}^{(3)}(n-1) + c_{j+3n}^{(3)}(n-1) \tag{10.12}$$

$$\begin{aligned} c_j^{(4)}(n) &= c_{j-4n}^{(4)}(n-1) + 4c_{j-2n}^{(4)}(n-1) + 6c_j^{(4)}(n-1) \\ &\quad + 4c_{j+2n}^{(4)}(n-1) + c_{j+4n}^{(4)}(n-1). \end{aligned} \tag{10.13}$$

In general, for m even one obtains the formula

$$c_j^{(m)}(n) = \sum_{k=1}^{m/2} \binom{m}{k} c_{j\pm 2kn}^{(m)}(n-1) + \binom{m}{m/2} c_j^{(m)}(n-1), \tag{10.14}$$

$$c_j^{(m)}(n) = \sum_{k=1}^{(m+1)/2} \binom{m}{2k-1} c_{j\pm(2k-1)n}^{(m)}(n-1). \tag{10.15}$$

when m is even or odd, respectively.

10.2.4 Associated integer sequences

Various integer sequences can be recovered from the coefficients of $F_{n,m}(z)$ given in formula (10.8). Of particular interest are the sequences $c_0^{(m)}(n)$, representing the constant term of $F_{n,m}(z)$. As seen in our paper [47], the sequences $c_j^{(m)}(n)$ obtainde for fixed values $j = 1,2,\ldots$ have an interesting combinatorial interpretation and importance.

The case $m = 1$

For $m = 1$, sequence $c_0^{(1)}(n)$ represents also the number of solutions at level n to the signum equation, which is A063865 in OEIS. More precisely, $c_0^{(1)}(n)$ is the number of ways of choosing $+$ and $-$ such that

$$\pm 1 \pm 2 \pm 3 \pm \cdots \pm n = 0,$$

sometimes denoted by $S(n) = c_0^{(1)}(n)$. This is in fact an old combinatorial problem also considered by S. Finch [114]. Computations show that $c_0^{(1)}(40) = 5830034720$ and $c_0^{(1)}(100) = 173102400594872501663378632 4$, hence the sequence terms seem to grow rather quickly.

Concerning its asymptotic behaviour, Andrica and Tomescu [40] conjectured the following asymptotic formula in 2002:

$$\lim_{\substack{n\to\infty \\ n\equiv 0 \text{ or } 3 (mod 4)}} \frac{S(n)}{\frac{2^n}{n\sqrt{n}}} = \sqrt{\frac{6}{\pi}}.$$

This was proved analytically in 2013 by B.D. Sullivan [245]. Extensions of this result will be discussed in the following sections.

For $m = 1$ and fixed values of n, the coefficients $\{c_j^{(1)}(n)\}_{j\geq 0}$ produce the following finite sequences:

$c_j^{(1)}(1)$: 0,1

$c_j^{(1)}(2)$: 0,1,0,1

$c_j^{(1)}(3)$: 2,0,1,0,1,0,1

$c_j^{(1)}(4)$: 2,0,2,0,2,0,1,0,1,0,1

$c_j^{(1)}(5)$: 0,3,0,3,0,3,0,2,0,2,0,1,0,1,0,1

$c_j^{(1)}(6)$: 0,5,0,5,0,4,0,4,0,4,0,3,0,2,0,2,0,1,0,1,0,1

$c_j^{(1)}(7)$: 8,0,8,0,8,0,7,0,7,0,6,0,5,0,5,0,4,0,3,0,2,0,2,0,1,0,1,0,1

$c_j^{(1)}(8)$: 14,0,13,0,13,0,13,0,12,0,11,0,10,0,9,0,8,0,7,0,6,0,5,0,4,
0,3,0,2,0,2,0,1,0,1,0,1

$c_j^{(1)}(9)$: 0,23,0,23,0,22,0,21,0,21,0,19,0,18,0,17,0,15,0,13,0,12,
0,10,0,9,0,8,0,6,0,5,0,4,0,3,0,2,0,2,0,1,0,1,0,1

Notice that $\{c_j^{(1)}(n)\}_{j\geq 0}$ has $n(n+1)/2+1$ relevant terms, i.e., $c_j^{(1)}(n) = 0$ for $j > n(n+1)/2+1$. The rows of this triangle are not indexed in the OEIS.

The case $m = 2$

For $m = 2$ one recovers the sequence

$$c_0^{(2)}(n) : 2,4,10,26,76,236,760,2522,8556,29504,\ldots,$$

indexed in OEIS as A047653. By the recurrence formula (10.9), one obtains

$$c_0^{(2)}(n) = \sum_{j\in\mathbb{Z}} c_j^{(1)}(n)c_j^{(1)}(n) = S^2(n) + 2\sum_{j=1}^{n(n+1)/2} (c_j^{(1)}(n))^2. \tag{10.16}$$

Concerning its asymptotic equivalent, the following formula was conjectured by Kotesovec in 2014 (see A047653 description in [211])

$$\lim_{n\to\infty} \frac{c_0^{(2)}(n)}{\frac{4^n}{n\sqrt{n}}} = \sqrt{\frac{3}{\pi}}.$$

The coefficients $\{c_j^{(2)}(n)\}_{j\geq 0}$ generate the following finite sequences:

$c_j^{(2)}(1)$: 2,0,1

$c_j^{(2)}(2)$: 4,0,3,0,2,0,1

$c_j^{(2)}(3)$: 10,0,8,0,7,0,6,0,3,0,2,0,1

$c_j^{(2)}(4)$: 26,0,24,0,22,0,20,0,16,0,12,0,9,0,6,0,3,0,2,0,1

$c_j^{(2)}(5)$: 76,0,73,0,70,0,65,0,58,0,51,0,42,0,34,0,26,0,20,0,14,0,9,0,6,0,3,0,2,0,1

$c_j^{(2)}(6)$: 236,0,231,0,224,0,215,0,200,0,184,0,166,0,144,0,124,0,106,0,86,0,69,0,54,0,40,0,30,0,22,0,14,0,9,0,6,0,3,0,2,0,1.

Notice that $\{c_j^{(2)}(n)\}_{j\geq 0}$ has $n(n+1)+1$ relevant terms, i.e., $c_j^{(2)}(n) = 0$ for $j > n(n+1)+1$. The rows of this triangle are not indexed in the OEIS.

The case $m = 3$

For $m = 3$ one obtains the sequence

$$c_0^{(3)}(n) : 0,0,62,332,0,0,80006,531524,0,0,173607568,\ldots,$$

indexed in OEIS as A124995. While several terms of this sequences have been computed, its asymptotic behaviour is not currently known. However, a conjecture based suggested by numerical calculations has been formulated in the following section.

The coefficients $\{c_j^{(3)}(n)\}_{j\geq 0}$ produce the following finite sequences:

$c_j^{(3)}(1)$: 0,3,0,1

$c_j^{(3)}(2)$: 0,12,0,10,0,6,0,3,0,1

$c_j^{(3)}(3)$: 62,0,57,0,51,0,43,0,30,0,21,0,13,0,6,0,3,0,1

$c_j^{(3)}(4)$: 332,0,327,0,309,0,278,0,243,0,204,0,161,0,123,0,90,
0,61,0,39,0,24,0,13,0,6,0,3,0,1

$c_j^{(3)}(5)$: 0,1974,0,1932,0,1851,0,1731,0,1587,0,1419,0,1242,0,1062,0,
882,0,717,0,566,0,435,0,324,0,233,0,162,0,108,0,
70,0,42,0,24,0,13,0,6,0,3,0,1.

One can notice that $\{c_j^{(3)}(n)\}_{j\geq 0}$ has $3n(n+1)/2+1$ relevant terms, i.e., $c_j^{(3)}(n)=0$ for $j>3n(n+1)/2+1$. The rows of this triangle are not currently indexed in the encyclopedia of integer sequences OEIS.

The case $m=4$

For $m=4$ one recovers the sequence

$$c_0^{(4)}(n) : 6,44,426,4658,55260,689508,8914872,\ldots,$$

indexed in OEIS as A124996. The asymptotic behaviour of this sequence is not currently known, but a conjecture based on numerical calculations is formulated in the following section.

The coefficients $\{c_j^{(4)}(n)\}_{j\geq 0}$ produce the following finite sequences:

$c_j^{(4)}(1)$: 6,0,4,0,1

$c_j^{(4)}(2)$: 44,0,40,0,31,0,20,0,10,0,4,0,1

$c_j^{(4)}(3)$: 426,0,408,0,372,0,320,0,251,0,188,0,130,0,80,
0,47,0,24,0,10,0,4,0,1

$c_j^{(4)}(4)$: 4658,0,4584,0,4380,0,4064,0,3650,0,3176,0,2680,0,2184,
0,1716,0,1304,0,952,0,664,0,445,0,284,0,170,0,96,0,
51,0,24,0,10,0,4,0,1

$c_j^{(4)}(5)$: 55260,0,54792,0,53433,0,51236,0,48302,0,44768,0,40773,0,
36492,0,32078,0,27692,0,23459,0,19492,0,15882,0,12672,0,
9902,0,7564,0,5642,0,4108,0,2912,0,2008,0,1342,0,868,0,
541,0,324,0,186,0,100,0,51,0,24,0,10,0,4,0,1

One can notice that $\{c_j^{(4)}(n)\}_{j\geq 0}$ has $2n(n+1)+1$ relevant terms, i.e., $c_j^{(4)}(n)=0$ for $j>2n(n+1)+1$. The rows of this triangle are not currently indexed in the encyclopedia of integer sequences OEIS and more research is required to study the interpretations.

10.2.5 Some conjectures

Numerical evidence suggests a number of conjectures.

10.2.5.1 Asymptotic behaviour of sequences $\{c_0^{(m)}(n)\}_{n\geq 0}$

In 2002, Andrica and Tomescu conjectured in the paper [40], the following asymptotic formula for $S(n)=c_0^{(1)}(n)$:

$$\lim_{\substack{n\to\infty \\ n\equiv 0 \text{ or } 3(mod 4)}} \frac{S(n)}{\frac{2^n}{n\sqrt{n}}}=\sqrt{\frac{6}{\pi}}.$$

This was proved in 2013 by using analytic methods by B.D. Sullivan [245].

The following asymptotic formula for $c_0^{(2)}(n)$ was then conjectured by Kotesovec in 2014 (see A047653 in [211]):

$$\lim_{n\to\infty} \frac{c_0^{(2)}(n)}{\frac{4^n}{n\sqrt{n}}}=\sqrt{\frac{3}{\pi}}.$$

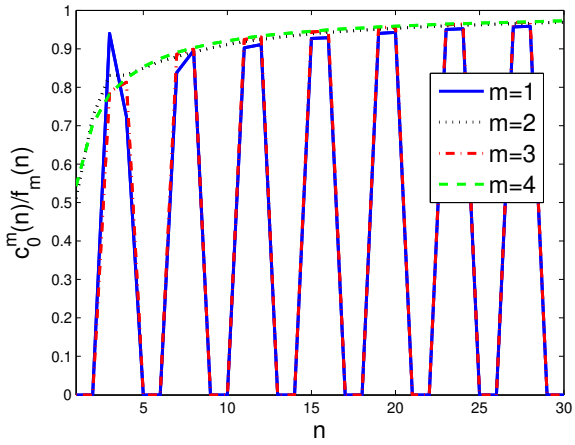

Fig. 10.1 First 30 terms of sequences $\frac{c_0^{(m)}(n)}{f_m(n)}$, $m = 1,2,3,4$, with $f_m(n)$ given by (10.17).

We aim to establish a more general result for $c_0^{(m)}(n)$. To this end, let $m,n \geq 1$ be integers and define the function

$$f_m(n) = \sqrt{\frac{6}{m\pi}} \frac{2^{mn}}{n\sqrt{n}}. \tag{10.17}$$

The numerical results obtained for $m = 1,2,3,4$ shown in Fig. 10.1, suggest the following asymptotic behaviour of $c_0^{(m)}(n)$.

Conjecture 10.1. Let $m \geq 1$ be an integer. The following formula holds

$$\lim_{n\to\infty} \frac{c_0^{(m)}(n)}{\frac{2^{mn}}{n\sqrt{n}}} = \sqrt{\frac{6}{m\pi}}. \tag{10.18}$$

10.2.5.2 On the properties of $c_j^m(n)$

Note that $\{c_j^{(m)}(n)\}_{j\geq 0}$ has $\frac{mn(n+1)}{2}+1$ relevant terms, i.e., $c_j^{(m)}(n) = 0$ for $j > \frac{mn(n+1)}{2}+1$, and we know that $\{c_j^{(1)}(n)\}_{j\in\mathbb{Z}}$ has a modulo 2 unimodality.

Numerical evidence obtained so far suggests two other conjectures.

Conjecture 10.2. The non-zero subsequence of $\{c_j^{(m)}(n)\}_{j\in\mathbb{Z}}$ is unimodal. As $c_j^{(m)}(n) = c_{-j}^{(m)}(n)$ and every second term is zero, it is sufficient to prove that

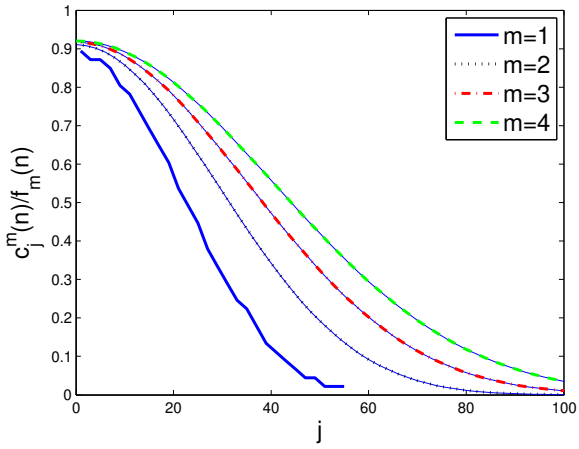

Fig. 10.2 Plot of $\frac{c_j^{(m)}(n)}{f_m(n)}$ evaluated for $n = 10$, $m = 1,2,3,4$, $j \in \{0,\ldots,\frac{mn(n+1)}{2}+1\}$, where the function $f_m(n)$ is given by (10.17).

the subsequences $\{c_{2j}^{(m)}(n)\}_{j\geq 0}$ and $\{c_{2j+1}^{(m)}(n)\}_{j\geq 0}$ are decreasing, by using formula (10.9).

The following behaviour is suggested by Fig 10.2.

Conjecture 10.3. For any integers $m,n \geq 1$, the coefficients $c_j^{(m)}(n)$ belong to a normally distribution shaped curve. If true, this conjecture would explain the unimodality of $c_j^{(m)}(n)$ for fixed m,n, as well as the asymptotic limits for $c_0^m(n)$ as n increases to infinity, for fixed m.

10.3 Ordered k-partitions of multisets

An important problem is the study of the number of partitions of multisets having certain properties. Results concerning the number of partitions of multisets, as well as asymptotic formulae for small multiplicity values were obtained in the 1970's by Bender [66] and Bender et al. [67]. For further information about multiset theory, one may consult Stanley's paper [243].

Some partition problems have important practical applications, as for example the famous strongly NP-complete problem related to 3-partitions. For the positive integers b,m and $a_1,\ldots,a_n$ such that $n = 3m$ and $\sum_{s=1}^{n} a_s = mb$, one needs to partition the set $\{a_1,\ldots,a_n\}$ into m subsets, each containing exactly three elements, whose sum is exactly b (see, e.g., [116] and [117]).

For example, the set $\{10,13,5,15,7,10\}$ can be partitioned into the two sets $\{10,13,7\}$, $\{5,15,10\}$, each of which sum to 30.

The key results in this section were published in [22], while the connections to Diophantine equations were explored in [26] and [27]. In 2023, He et al. [131] proved the uniformly asymptotic formula conjectured in [22]. In 2024, Zeenath et al. [265] used the notion of k-partitions with equal sums proposed in [22] and extended the techniques to give an explicit formula for counting and constructing the balanced rotation symmetric Boolean functions applied in cryptography, closing an important open problem which lasted a few decades.

10.3.1 Notations and basic formulae

Let $\alpha_1,\ldots,\alpha_n$ be real numbers, $m_1,\ldots,m_n$ positive integers. For the multiset

$$M=\{\underbrace{\alpha_1,\cdots,\alpha_1}_{m_1\ times},\cdots,\underbrace{\alpha_n,\cdots,\alpha_n}_{m_n\ times}\},$$

the number m_s is called the **multiplicity** of the element α_s, $s=1,\ldots,n$, while $\sigma(M)=\sum_{s=1}^{n} m_s\alpha_s$ represents the **sum** of the elements of M. For a simplified notation, we shall denote $\mathbf{m}=(m_1,\ldots,m_n)$ and $\boldsymbol{\alpha}=(\alpha_1,\ldots,\alpha_n)$.

Definition 10.2. Let $k\geq 2$ be an integer. Denote by $S_k(\mathbf{m};\boldsymbol{\alpha})$ the number of ordered k-partitions of M having equal sums, i.e., the number of k-tuples $(C_1,\ldots,C_k)$ of subsets of pairwise disjoint subsets of M such that

(i) $C_1\cup\cdots\cup C_k=M$;

(ii) $\sigma(C_1)=\cdots=\sigma(C_k)=\frac{1}{k}\sigma(M)$.

Clearly, one has the relationship $S_k(\mathbf{m};\boldsymbol{\alpha})=k!\,N_k(\mathbf{m};\boldsymbol{\alpha})$, where $N_k(\mathbf{m};\boldsymbol{\alpha})$ is the number of non-ordered k-partitions of M.

The number $S_k(\mathbf{m};\boldsymbol{\alpha})$ is the constant term of the expansion of a Laurent polynomial $F(X_1,\ldots,X_{k-1})\in\mathbb{Z}[X_1,\ldots,X_{k-1},X_1^{-1},\ldots,X_{k-1}^{-1}]$, defined by

$$F(X_1,\ldots,X_{k-1})=\prod_{s=1}^{n}\left(X_1^{\alpha_s}+\cdots+X_{k-1}^{\alpha_s}+\frac{1}{(X_1\cdots X_{k-1})^{\alpha_s}}\right)^{m_s}. \tag{10.19}$$

Indeed, assume that for $s=1,\ldots,n$, from $\left(X_1^{\alpha_s}+\cdots+X_{k-1}^{\alpha_s}+\frac{1}{(X_1\cdots X_{k-1})^{\alpha_s}}\right)^{m_s}$ we have selected c_j^s terms equal to $X_j^{\alpha_s}$, with $j=1,\ldots,k-1$, and c_k^s terms equal to $\frac{1}{(X_1\cdots X_{k-1})^{\alpha_s}}$. Notice that we must have $c_1^s+\cdots+c_k^s=m_s$.

Such a selection contributes to the free term if and only if

$$X_1^{\sum_{s=1}^n c_1^s \alpha_s} \cdots X_{k-1}^{\sum_{s=1}^n c_{k-1}^s \alpha_s} \cdot \frac{1}{(X_1 \cdots X_{k-1})^{\sum_{s=1}^n c_k^s \alpha_s}} = 1,$$

which is equivalent to $\sum_{s=1}^n c_1^s \alpha_s = \cdots = \sum_{s=1}^n c_{k-1}^s \alpha_s = \sum_{s=1}^n c_k^s \alpha_s$.

This means that the sets

$$C_j = \{\underbrace{\alpha_1, \ldots, \alpha_1}_{c_j^1 \text{ times}}, \ldots, \underbrace{\alpha_n, \ldots, \alpha_n}_{c_j^n \text{ times}}\}, \quad j = 1,2,\ldots,k,$$

represent a partition of M which also satisfies property (ii) in Definition 10.2.

10.3.2 An integral formula

Ordering (10.19) after the integer powers of X_j, for $j = 1,\ldots,k-1$, one has

$$F(X_1,\ldots,X_{k-1}) = \sum_{m\in\mathbb{Z}} P_{m,j}(X_1,\ldots,X_{j-1},X_{j+1},\ldots,X_{k-1}) X_j^m, \tag{10.20}$$

where $P_{m,j}(X_1,\ldots,X_{j-1},X_{j+1},\ldots,X_{k-1})$ are Laurent polynomials. As F is symmetric in its variables, the polynomials $P_{m,j}$ are independent of j, hence we may use the simplified notation $P_m(X_1,\ldots,X_{j-1},X_{j+1},\ldots,X_{k-1})$, and the free term of $F(X_1,\ldots,X_{k-1})$ is the free term of $P_0(X_1,\ldots,X_{j-1},X_{j+1},\ldots,X_{k-1})$.

Denoting by $\widetilde{X}_j = (X_1,\ldots,X_{j-1},X_{j+1},\ldots,X_{k-1})$ for simplicity, we have

$$F(X_1,\ldots,X_{k-1}) = \prod_{s=1}^n \left(X_1^{\alpha_s} + \cdots + X_{k-1}^{\alpha_s} + \frac{1}{(X_1\cdots X_{k-1})^{\alpha_s}} \right)^{m_s} \tag{10.21}$$

$$= P_0(\widetilde{X}_j) + \sum_{m\in\mathbb{Z}, m\neq 0} P_m(\widetilde{X}_j) X_j^m. \tag{10.22}$$

Let $X_j = \cos t + i \sin t$ in (10.21) and integrate with respect to t over $[0,2\pi]$. Since the integral of the monomial X_j^m with respect to t over $[0,2\pi]$ vanishes for $m \neq 0$, the integral representation of the polynomial is given by

$$P_0(\widetilde{X}_j) = \frac{1}{2\pi} \int_0^{2\pi} \prod_{s=1}^n \left(X_1^{\alpha_s} + \cdots + X_{k-1}^{\alpha_s} + \frac{1}{(X_1\cdots X_{k-1})^{\alpha_s}} \right)^{m_s} \mathrm{d}t. \tag{10.23}$$

Setting $X_j = X$, $X_l = 1$ for $l = 1,\ldots,k-1$ and $l \neq j$ in (10.21), one obtains

$$\prod_{s=1}^n \left(X^{\alpha_s} + k - 2 + \frac{1}{X^{\alpha_s}} \right)^{m_s} = P_0(1,\ldots,1) + \sum_{m\in\mathbb{Z}, m\neq 0} P_m(1,\ldots,1) X^m. \tag{10.24}$$

By symmetry in X and X^{-1} we have

$$P_m(1,\dots,1) = P_{-m}(1,\dots,1), \quad m \in \mathbb{Z}.$$

Also, from (10.23) we deduce that

$$P_0(1,\dots,1) = \frac{1}{2\pi}\int_0^{2\pi} \prod_{s=1}^{n} \left(X^{\alpha_s} + k - 2 + \frac{1}{X^{\alpha_s}} \right)^{m_s} \mathrm{d}t. \tag{10.25}$$

Note that $P_0(1,\dots,1)$ depends on k, $\mathbf{m}$ and $\boldsymbol{\alpha}$.

Since $X^{\alpha_s} + \frac{1}{X^{\alpha_s}} = 2\cos\alpha_s t$, we have the following relation

$$Q_k(\mathbf{m};\boldsymbol{\alpha}) := P_0(1,\dots,1) = \frac{1}{2\pi}\int_0^{2\pi} \prod_{s=1}^{n} (k - 2 + 2\cos\alpha_s t)^{m_s}\, \mathrm{d}t. \tag{10.26}$$

We have that

$$Q_k(\mathbf{m};\boldsymbol{\alpha}) = S_k(\mathbf{m};\boldsymbol{\alpha}) + R_k(\mathbf{m};\boldsymbol{\alpha}), \tag{10.27}$$

where $R_k(\mathbf{m};\boldsymbol{\alpha})$ is the sum of the coefficients of $P_0(\widetilde{X_j})$, different from the free term. Also, setting $X = 1$ in (10.24) we get $k^{m_1+\cdots+m_n} = \sum_{m\in\mathbb{Z}} P_m(1\dots,1)$, that is the sum of all the coefficients in all polynomials P_m is $k^{m_1+\cdots+m_n}$.

By formula (10.26), after simple computations it follows that

$$Q_4(\mathbf{m};\boldsymbol{\alpha}) = Q_2\left(2\mathbf{m};\frac{\boldsymbol{\alpha}}{2}\right).$$

As shown in [47], the integral formula for the number of ordered 2-partitions with equal sum of the multiset M is

$$c_0(\mathbf{m};\boldsymbol{\alpha}) = S_2(\mathbf{m};\boldsymbol{\alpha}) = \frac{2^{m_1+\cdots+m_n}}{2\pi}\int_0^{2\pi} \prod_{s=1}^{n} (\cos\alpha_s t)^{m_s}\, \mathrm{d}t, \tag{10.28}$$

which for $m_1 = \cdots = m_n = m$ and $\alpha_s = s$, $s = 1,\dots,n$, produces the formula

$$c_0^{(m)}(n) = \frac{2^{nm}}{2\pi}\int_0^{2\pi} \prod_{s=1}^{n} (\cos st)^m\, \mathrm{d}t. \tag{10.29}$$

If $Q_k(n) = Q_k(1,\dots,1;1,2,\dots,n)$, then $Q_2(n) = c_0^{(1)}(n)$ and $Q_4(n) = c_0^{(2)}(n)$.

10.3.3 k-partitions with equal sums of the set $\{1,\dots,n\}$

In this section we set $\alpha_s = s$ and $m_s = 1$, for $s = 1,\dots,n$ and use the simplified notations $S_k(n)$ for $S_k(\mathbf{m};\boldsymbol{\alpha})$ and $R_k(n)$ for $R_k(\mathbf{m};\boldsymbol{\alpha})$. Some recurrences can be obtained for the coefficients of the polynomial $F(X_1,\dots,X_{k-1})$ defined by

(10.19), which is indexed by the level n, as in the formula

$$F_n(X_1,\dots,X_{k-1}) = \prod_{s=1}^{n}\left(X_1^s+\cdots+X_{k-1}^s+\frac{1}{(X_1\cdots X_{k-1})^s}\right). \tag{10.30}$$

We first write $F_n(X_1,\dots,X_{k-1})$ as a Laurent polynomial in $X_1,\dots,X_{k-1}$ with integer coefficients, given by he formula

$$F_n(X_1,\dots,X_{k-1}) = \sum_{j_1,\dots,j_{k-1}\in\mathbb{Z}} c_{j_1,\dots,j_{k-1}}(n)X_1^{j_1}X_2^{j_2}\cdots X_{k-1}^{j_{k-1}}. \tag{10.31}$$

Clearly, we have $F_n(X_1,\dots,X_{k-1}) = \frac{U(X_1,\dots,X_{k-1})}{V(X_1,\dots,X_{k-1})}$, where U and V are polynomials. If $V\neq 0$ at the origin of $\mathbb{R}^{k-1}$, then the coefficients in (10.31) are given by the Cauchy integral formula

$$c_{j_1,\dots,j_{k-1}(n)} = \frac{1}{(2\pi i)^{k-1}}\int_T \frac{F_n(X_1,\dots,X_{k-1})}{x_1\cdots x_{k-1}}x_1^{-j_1}\cdots x_{k-1}^{-j_{k-1}}\mathrm{d}x_1\wedge\cdots\wedge\mathrm{d}x_{k-1}, \tag{10.32}$$

with T a product of sufficiently small circles around the coordinate axes of $\mathbb{R}^{k-1}$. While this is a closed formula, for effective computations it is more practical to use a recurrence between the coefficients of levels n and $n-1$.

Theorem 10.1. *Denote by* $\mathbf{e_1},\dots,\mathbf{e_{k-1}}$ *the vectors of the canonical basis in* $\mathbb{Z}^{k-1}$. *The following recurrence relation is valid for* $\mathbf{j}=(j_1,\dots,j_{k-1})\in\mathbb{Z}^{k-1}$ *and* $n\geq 1$*:*

$$c_{\mathbf{j}}(n) = c_{\mathbf{j}-n\mathbf{e_1}}(n-1)+\cdots+c_{\mathbf{j}-n\mathbf{e_{k-1}}}(n-1)+c_{\mathbf{j}+n(1,\dots,1)}(n-1). \tag{10.33}$$

Proof. Indeed, by formula (10.30) we obtain

$$\begin{aligned}
F_n(X_1,\dots,X_{k-1}) &= F_{n-1}(X_1,\dots,X_{k-1})\left(X_1^n+\cdots+X_{k-1}^n+\frac{1}{(X_1X_2\cdots X_{k-1})^n}\right)\\
&= \left(\sum_{\mathbf{j}\in\mathbb{Z}^{k-1}} c_{\mathbf{j}}(n-1)X_1^{j_1}\cdots X_{k-1}^{j_{k-1}}\right)\left(X_1^n+\cdots+X_{k-1}^n+\frac{1}{(X_1\cdots X_{k-1})^n}\right)\\
&= \sum_{\mathbf{j}\in\mathbb{Z}^{k-1}} c_{\mathbf{j}}(n-1)\left(X_1^{j_1+n}\cdots X_{k-1}^{j_{k-1}}+\cdots+X_1^{j_1}\cdots X_{k-1}^{j_{k-1}+n}+X_1^{j_1-n}\cdots X_{k-1}^{j_{k-1}-n}\right)\\
&= \sum_{\mathbf{j}\in\mathbb{Z}^{k-1}}\left(c_{\mathbf{j}-n\mathbf{e_1}}(n-1)+\cdots+c_{\mathbf{j}-n\mathbf{e_{k-1}}}(n-1)+c_{\mathbf{j}+n(1,\dots,1)}(n-1)\right)X_1^{j_1}\cdots X_{k-1}^{j_{k-1}}.
\end{aligned}$$

□

For each $j\in\{1,\dots,k-1\}$, we write F_n as a Laurent polynomial in X_j as

$$F_n(X_1,\dots,X_{k-1}) = \sum_{m\in\mathbb{Z}} P_{n,m,j}(\widetilde{X_j})X_j^m, \tag{10.34}$$

where $\widetilde{X}_j = (X_1,\dots,X_{j-1},X_{j+1},\dots,X_{k-1})$. Since $F_n(X_1,\dots,X_{k-1})$ is symmetric, the coefficients $P_{n,m,j}$ are independent of j, so the simplified notation $P_{n,m}(\widetilde{X_j})$ can be used. These polynomials can be obtained recursively.

Theorem 10.2. *The recurrence below holds for $m\in\mathbb{Z}$, $j=1,\dots,k-1$ and $n\geq 1$.*

$$P_{n,m}(\widetilde{X_j}) = P_{n-1,m-n}(\widetilde{X_j}) + \Big(\sum_{p\neq j} X_p^n\Big)P_{n-1,m}(\widetilde{X_j}) + \Big(\prod_{p\neq j} X_p\Big)^{-n} P_{n-1,m+n}(\widetilde{X_j}).$$

Also, for $m=0$ we have

$$P_{n,0}(\widetilde{X_j}) = P_{n-1,-n}(\widetilde{X_j}) + \Big(\sum_{p\neq j} X_p^n\Big)P_{n-1,0}(\widetilde{X_j}) + \Big(\prod_{p\neq j} X_p\Big)^{-n} P_{n-1,n}(\widetilde{X_j}). \tag{10.35}$$

Proof. The following formula can be established.

$$\begin{aligned}
F_n(X_1,\dots,X_{k-1}) &= F_{n-1}(X_1,\dots,X_{k-1})\left(X_1^n+\cdots+X_{k-1}^n+\frac{1}{(X_1\cdots X_{k-1})^n}\right)\\
&= \left(\sum_{m\in\mathbb{Z}} P_{n-1,m}(\widetilde{X_j})X_j^m\right)\left(X_1^n+\cdots+X_{k-1}^n+\frac{1}{(X_1\cdots X_{k-1})^n}\right)\\
&= \sum_{m\in\mathbb{Z}} [P_{n-1,m-n}(\widetilde{X_j}) + \Big(\sum_{p\neq j} X_p^n\Big)P_{n-1,m}(\widetilde{X_j}) + \Big(\prod_{p\neq j} X_p\Big)^{-n} P_{n-1,m+n}(\widetilde{X_j})]X_j^m.
\end{aligned}$$

Substituting $m=0$ into this formula, we obtain (10.35). □

Setting $X_1 = X$ and $X_p = 1$ for $p = 2,\dots,k-1$ in (10.30), one obtains

$$F_n(X,1,\dots,1) = \prod_{s=1}^{n}\left(X^s+k-2+\frac{1}{X^s}\right) = \sum_{m\in\mathbb{Z}} P_{n,m}(1,\dots,1)X^m. \tag{10.36}$$

Notice that $P_{n,m}(1,\dots,1) = P_{n,-m}(1,\dots,1)$, $m\in\mathbb{Z}$, which represents the sum of the coefficients of the Laurent polynomial $P_{n,m}(X_1,\dots,X_{k-1})$. For simplicity, we denote $P_{n,m} := P_{n,m}(1,\dots,1)$. The terms of the sequence $\{P_{n,0}\}_{n\geq 1}$ can be obtained from the following double recurrence:

$$P_{n,0} = P_{n-1,-n} + P_{n-1,0} + P_{n-1,n} = P_{n-1,0} + 2P_{n-1,n}. \tag{10.37}$$

From the integral formula (10.26) applied in this case, we can also compute the terms $P_{n,0}$ directly. Since this computation is actually performed for a given value of k, for what follows we introduce the notation

$$Q_k(n) = P_{n,0} = S_k(n) + R_k(n) = \frac{1}{2\pi}\int_0^{2\pi}\prod_{s=1}^{n}(k-2+2\cos st)\,\mathrm{d}t. \quad (10.38)$$

10.3.4 Numerical examples and integer sequences

In we analyze some numerical examples for $S_k(n)$, $R_k(n)$ and $Q_k(n)$. In this process we provide new context for a number of existing sequences, and identify novel entries to OEIS. We then establish a polynomial formula for $Q_k(n)$ and conjecture its asymptotic behaviour. We also conjecture properties related to the distribution of perfect powers within this sequence.

10.3.4.1 Integer sequences related to $S_k(n)$ and k-partitions of multisets

Denoting by $T(n,k)$ the number of set partitions of $[n]$ into k blocks with equal element sum, this is indexed since 2016 in OEIS as a triangle A275714. We have $S_k(n) = k! \cdot T(n,k)$.

Example 10.1. *$S_3(n)$ has been recently added by us to OEIS as A317577 :*

$$0,0,0,0,6,6,0,18,54,0,258,612,0,3570,8880,0,55764,142368,0,947946,$$
$$2468844,0,17099808,45375498,0,323927184,871038570,0,\ldots.$$

For $n = 3k+1$, the number $\frac{n(n+1)}{2}$ is not divisible by 3, hence $S_3(n) = 0$. Also, $S_3(n) = 6 \cdot a(n)$, where $a(n)$ is the sequence A112972 in OEIS.

Example 10.2. *For $k = 4$, the free term $S_4(n)$ produces a new OEIS sequence:*

$$0,0,0,0,0,0,24,24,0,0,0,0,0,0,20904,63600,0,0,0,0,0,0,227090256,\ldots.$$

For $n \neq 8k-1, 8k$, the number $\frac{n(n+1)}{2}$ is not divisible by 4, hence $S_4(n) = 0$.

Example 10.3. *For $k = 5$, the free term $S_5(n)$ produces a new OEIS sequence:*

$$0,0,0,0,0,0,0,0,120,120,0,0,0,8160,22440,0,0,0,3331560,13021920,0,\ldots.$$

For $n \neq 5k-1, 5k$, the number $\frac{n(n+1)}{2}$ is not divisible by 5, hence $S_5(n) = 0$.

10.3.4.2 Integer sequences related to $Q_k(n)$ and the 3-signum equation

We now investigate the expression $Q_k(n)$ defined by (10.38). In particular, $Q_3(n)$ gives the number of solutions of the 3-signum equation [15]

$$1\cdot\varepsilon_1+2\cdot\varepsilon_2+\cdots+n\cdot\varepsilon_n=0, \tag{10.39}$$

where $\varepsilon_s\in\{-1,0,1\}$, $s=1,\ldots,n$. Below we study some properties of this sequence and we illustrate a counting procedure for $Q_k(n)$ when $k=3$, $k=4$ and $k=5$. We then highlight some novel integer sequences.

The following result provides a new combinatorial context for $Q_k(n)$.

Theorem 10.3. *A formula for $Q_k(n)$ is given by the number of ordered partitions of $[n]$ into k disjoint sets $A_1,\ldots,A_k$, with the property $\sigma(A_1)=\sigma(A_k)$.*

Proof. A monomial $X_1^{d_1}\cdots X_{k-1}^{d_{k-1}}(X_1\cdots X_{k-1})^{-d_k}$ of $F_n(X_1,\ldots,X_{k-1})$ in (10.30) is independent of X_1 if and only if $d_1=d_k$. The number of such monomials equals the number the ordered partitions $A_1,A_2,\ldots,A_k$ of $[n]$ such that $\sigma(A_1)=\sigma(A_k)=d_1$, with $d_j\geq 0$ for $j=1,\ldots,k$ and $d_1+\cdots+d_k=\sigma([n])$. □

Example 10.4. *For $k=3$, the sequence $Q_3(n)$ starts with the terms*

$$1,1,3,7,15,35,87,217,547,1417,3735,9911,26513,71581,194681,532481,\ldots.$$

and is indexed in the OEIS as A007576. Same terms are obtained from

$$Q_3(n)=\frac{1}{2\pi}\int_0^{2\pi}\prod_{s=1}^{n}(1+2\cos st)\,\mathrm{d}t. \tag{10.40}$$

It was recently conjectured (see context for A007576 in OEIS [211]) that

$$Q_3(n)\sim\frac{1}{2\sqrt{\pi}}\cdot\frac{3^{n+1}}{n^{3/2}}.$$

As the monomials in the $F_n(X,Y)$ expansion have the form $X^{\alpha}Y^{\beta}(XY)^{-\gamma}$, a term is independent of X if and only if $\alpha=\gamma$. To identify the numbers of terms independent of X, we count all subsets A and B of $\{1,2,\ldots,n\}$ such that $A\cap B=\emptyset$ with $\sigma(A)=\sigma(B)=\alpha$ with $\alpha,\beta,\gamma\geq 0$ and $\alpha+\beta+\gamma=\sigma([n])$. This is equivalent to finding the number of solutions of the 3-signum equation (10.39). For $k=3$ we list below the triples obtained for $n=4$ and $n=5$.

When $[n]=\{1,2,3,4\}$, we have $\sigma([n])=10$. We enumerate the partitions A,B,C of $[n]$ having the property $\sigma(A)=\sigma(C)$. The problem is equivalent to finding all the triplets (α,β,γ) such that $\alpha,\beta,\gamma\geq 0$, $\alpha=\gamma$ and $\alpha+\beta+\gamma=10$. Table 10.1 presents all such partitions and ε_s, $s=1,\ldots,4$, satisfying (10.39). Adding the multiplicities we confirm that $Q_3(4)=7$.

When $[n]=\{1,2,3,4,5\}$, we have $\sigma([n])=15$. We count the partitions A,B,C of $[n]$ such that $\sigma(A)=\sigma(C)$. To this end we find the number of triplets (α,β,γ) such that $\alpha,\beta,\gamma\geq 0$, $\alpha=\gamma$ and $\alpha+\beta+\gamma=15$. From simple

α	β	γ	A	B	C	ε_1	ε_2	ε_3	ε_4	Multiplicity
0	10	0	$\emptyset$	$[n]$	$\emptyset$	0	0	0	0	1
3	4	3	{1,2}	{4}	{3}	1	1	-1	0	1
			{3}	{4}	{1,2}	-1	-1	1	0	1
4	2	4	{1,3}	{2}	{4}	1	0	1	-1	1
			{4}	{2}	{1,3}	-1	0	-1	1	1
5	5	5	{1,4}	$\emptyset$	{2,3}	1	-1	-1	1	1
			{2,3}	$\emptyset$	{1,4}	-1	1	1	-1	1

Table 10.1 Partitions of $[n]$ into k subsets when $n = 4$ and $k = 3$. $Q_3(n) = 7$ for $n = 4$.

computations we obtain Table 10.2 presenting all possible subset configurations, along with the corresponding values for ε_s, $s = 1,\ldots,5$, which feature in (10.39). Adding the multiplicities one may confirm that $Q_3(5) = 15$.

α	β	γ	A	B	C	ε_1	ε_2	ε_3	ε_4	ε_5	Multiplicity
0	15	0	$\emptyset$	$[n]$	$\emptyset$	0	0	0	0	0	1
3	9	3	{1,2}	{4,5}	{3}	1	1	-1	0	0	1
			{3}	{4,5}	{1,2}	-1	-1	1	0	0	1
4	7	4	{1,3}	{2,5}	{4}	1	0	1	-1	0	1
			{4}	{2,5}	{1,3}	-1	0	-1	1	0	1
5	5	5	{1,4}	{2,3}	{5}	1	0	0	1	-1	1
			{5}	{2,3}	{1,4}	-1	0	0	-1	1	1
			{2,3}	{1,4}	{5}	0	1	1	0	-1	1
			{5}	{1,4}	{2,3}	0	-1	-1	0	1	1
			{1,4}	{5}	{2,3}	1	-1	-1	1	0	1
			{2,3}	{5}	{1,4}	-1	1	1	-1	0	1
6	3	6	{1,5}	{3}	{2,4}	1	-1	0	-1	1	1
			{2,4}	{3}	{1,5}	-1	1	0	1	-1	1
7	1	7	{2,5}	{1}	{3,4}	0	1	-1	-1	1	1
			{3,4}	{1}	{2,5}	0	-1	1	1	-1	1

Table 10.2 Partitions of $[n]$ into k subsets when $n = 5$ and $k = 3$. $Q_3(n) = 15$ for $n = 5$.

Example 10.5. *The sequence $Q_4(n)$ (A047653 in OEIS) starts with*

$$2,4,10,26,76,236,760,2522,8556,29504,103130,364548,1300820,$$

for which we also give the a new integral formula

$$Q_4(n) = \frac{1}{2\pi}\int_0^{2\pi}\prod_{s=1}^{n}(2+2\cos st)\,\mathrm{d}t = \frac{2^{2n}}{2\pi}\int_0^{2\pi}\prod_{s=1}^{n}\cos^2\frac{st}{2}\,\mathrm{d}t. \qquad (10.41)$$

An asymptotic expansion was conjectured in 2014 (see A047653 in [211])

$$Q_4(n) \sim \sqrt{\frac{3}{\pi}} \cdot \frac{4^n}{n^{3/2}}.$$

The sequence $R_4(n)$ is also novel, and begins with the numbers

$$2,4,10,26,76,236,736,2498,8556,29504,103130,364548,1300820,$$
$$4679472,16931258,61726842,\ldots$$

Count the partitions A,B,C,D of $\{1,2,3,4,5\}$ such that $\sigma(A) = \sigma(D)$, that is the number of 4-tuples $(\alpha,\beta,\gamma,\delta)$ with the properties $\alpha,\beta,\gamma,\delta \geq 0$, $\alpha = \delta$ and $\alpha+\beta+\gamma+\delta = 15$. Direct computations give the values in Table 10.3.

α	$\beta+\gamma$	δ	A	$B\cup C$	D	ε_1	ε_2	ε_3	ε_4	ε_5	Multiplicity
0	15	0	$\emptyset$	$[n]$	$\emptyset$	0	0	0	0	0	2^5
3	9	3	$\{1,2\}$	$\{4,5\}$	$\{3\}$	1	1	-1	0	0	2^2
			$\{3\}$	$\{4,5\}$	$\{1,2\}$	-1	-1	1	0	0	2^2
4	7	4	$\{1,3\}$	$\{2,5\}$	$\{4\}$	1	0	1	-1	0	2^2
			$\{4\}$	$\{2,5\}$	$\{1,3\}$	-1	0	-1	1	0	2^2
5	5	5	$\{1,4\}$	$\{2,3\}$	$\{5\}$	1	0	0	1	-1	2^2
			$\{5\}$	$\{2,3\}$	$\{1,4\}$	-1	0	0	-1	1	2^2
			$\{2,3\}$	$\{1,4\}$	$\{5\}$	0	1	1	0	-1	2^2
			$\{5\}$	$\{1,4\}$	$\{2,3\}$	0	-1	-1	0	1	2^2
			$\{1,4\}$	$\{5\}$	$\{2,3\}$	1	-1	-1	1	0	2
			$\{2,3\}$	$\{5\}$	$\{1,4\}$	-1	1	1	-1	0	2
6	3	6	$\{1,5\}$	$\{3\}$	$\{2,4\}$	1	-1	0	-1	1	2
			$\{2,4\}$	$\{3\}$	$\{1,5\}$	-1	1	0	1	-1	2
7	1	7	$\{2,5\}$	$\{1\}$	$\{3,4\}$	0	1	-1	-1	1	2
			$\{3,4\}$	$\{1\}$	$\{2,5\}$	0	-1	1	1	-1	2

Table 10.3 Partitions of $[n]$ into k subsets when $n = 5$ and $k = 4$. $Q_4(n) = 76$ for $n = 5$.

One may notice that $Q_4(5) = 76 = 2^5 + 8 \cdot 2^2 + 6 \cdot 2$.

Remark. In Table 10.3, the $B \cup C$ column contains all elements just once. There are 8 instances where this contains two elements, and then finally, 6 instances where this only has a single element. This suggest the formula

$$Q_k(5) = (k-2)^5 + 8(k-2)^2 + 6(k-2), \quad (k \geq 2) \tag{10.42}$$

which will be fully explained by Theorem 10.4.

Example 10.6. *The sequence $Q_5(n)$ produces the new integer sequence*

$$3,9,29,95,333,1215,4661,18509,76281,321729,1386757,6070591,\ldots.$$

First, observe that $3^5 + 8 \cdot 3^2 + 6 \cdot 3 = 333 = Q_5(5)$, *in accordance with* (10.42).

We count partitions A, B, C, D, E *of* $\{1,2,3,4,5,6\}$ *such that* $\sigma(A) = \sigma(E)$, *that is the number of 5-tuples* $(\alpha, \beta, \gamma, \delta, \epsilon)$ *such that* $\alpha, \beta, \gamma, \delta, \epsilon \geq 0$, $\alpha = \epsilon$ *and* $\alpha + \beta + \gamma + \delta + \epsilon = 21$. *Simple computations give the values in Table 10.4.*

α	$\sum\beta$	ϵ	A	$\cup B$	E	ε_1	ε_2	ε_3	ε_4	ε_5	ε_6	Mult.
0	21	0	$\emptyset$	$[n]$	$\emptyset$	0	0	0	0	0	0	3^6
3	15	3	{1,2}	{4,5,6}	{3}	1	1	-1	0	0	0	3^3
			{3}	{4,5,6}	{1,2}	-1	-1	1	0	0	0	3^3
4	13	4	{1,3}	{2,5,6}	{4}	1	0	1	-1	0	0	3^3
			{4}	{2,5,6}	{1,3}	-1	0	-1	1	0	0	3^3
5	11	5	{1,4}	{2,3,6}	{5}	1	0	0	1	-1	0	3^3
			{5}	{2,3,6}	{1,4}	-1	0	0	-1	1	0	3^3
			{2,3}	{1,4,6}	{5}	0	1	1	0	-1	0	3^3
			{5}	{1,4,6}	{2,3}	0	-1	-1	0	1	0	3^3
			{1,4}	{5,6}	{2,3}	1	-1	-1	1	0	0	3^2
			{2,3}	{5,6}	{1,4}	-1	1	1	-1	0	0	3^2
6	9	6	{1,5}	{2,3,4}	{6}	1	0	0	0	1	-1	3^3
			{6}	{1,3,5}	{1,5}	-1	0	0	0	-1	1	3^3
			{2,4}	{1,3,5}	{6}	0	1	0	1	0	-1	3^3
			{6}	{1,3,5}	{2,4}	0	-1	0	-1	0	1	3^3
			{1,2,3}	{4,5}	{6}	1	1	1	0	0	-1	3^2
			{6}	{4,5}	{1,2,3}	-1	-1	-1	0	0	1	3^2
			{1,5}	{3,6}	{2,4}	1	-1	0	-1	1	0	3^2
			{2,4}	{3,6}	{1,5}	-1	-1	0	-1	1	0	3^2
7	7	7	{1,6}	{3,4}	{2,5}	1	-1	0	0	-1	1	3^2
			{2,5}	{3,4}	{1,6}	-1	1	0	0	1	-1	3^2
			{1,6}	{2,5}	{3,4}	1	0	-1	-1	0	1	3^2
			{3,4}	{2,5}	{1,6}	-1	0	1	1	0	-1	3^2
			{2,5}	{1,6}	{3,4}	0	1	-1	-1	1	0	3^2
			{3,4}	{1,6}	{2,5}	0	-1	1	1	-1	0	3^2
8	5	8	{2,6}	{1,4}	{3,5}	0	1	-1	0	-1	1	3^2
			{3,5}	{1,4}	{2,6}	0	-1	1	0	1	-1	3^2
			{2,6}	{5}	{1,3,4}	-1	1	-1	-1	0	1	3^1
			{1,3,4}	{5}	{2,6}	1	-1	1	1	0	-1	3^1
9	3	9	{3,6}	{1,2}	{4,5}	0	0	1	-1	-1	1	3^2
			{4,5}	{1,2}	{3,6}	0	0	-1	1	1	-1	3^2
			{4,5}	{3}	{1,2,6}	-1	-1	0	1	1	-1	3^1
			{1,2,6}	{3}	{4,5}	1	1	0	-1	-1	1	3^1
10	1	10	{4,6}	{1}	{2,3,5}	0	-1	-1	1	-1	1	3^1
			{2,3,5}	{1}	{4,6}	0	1	1	-1	1	-1	3^1

Table 10.4 Partitions of $[n]$ into k subsets when $n = 6$ and $k = 5$. $Q_5(n) = 1215$ for $n = 6$.

Notice that we have $Q_5(6) = 1215 = 3^6 + 12 \cdot 3^3 + 16 \cdot 3^2 + 6 \cdot 3$ for $n = 6$.

Remark. In Table 10.4, the union $B \cup C \cup D$ contains all elements once. In 12 instances it contains three elements, in 16 it contains two elements, and in 6 it only has one element. This suggests a formula for $Q_k(6)$, $k \geq 2$:

$$Q_k(6) = (k-2)^6 + 12(k-2)^3 + 16(k-2)^2 + 6(k-2). \tag{10.43}$$

Tables 10.1 and 10.2 also inspire formulae for $Q_k(3)$ and $Q_k(4)$:

$$Q_k(3) = (k-2)^3 + 2, \quad Q_k(4) = (k-2)^4 + 4(k-2) + 2. \tag{10.44}$$

An enumerative formula for $Q_k(n)$ is given by the following result.

Theorem 10.4. 1° *The following formula holds*

$$Q_k(n) = \sum_{d=0}^{n} N(d,n) \cdot (k-2)^{n-d},$$

where for each $d = 0,\dots,n$, and $N(d,n)$ is the number of ordered partitions of $[n]$ into 3 subsets A,B,C, such that the cardinality of B is d and $\sigma(A) = \sigma(C)$.

2° *If $\sigma_d(\cos t, \cos 2t, \dots, \cos nt)$ represents the d-th symmetric sum of the terms $\cos t, \cos 2t, \dots, \cos nt$, then the coefficients $N(d,n)$ are given by the formula*

$$N(d,n) = \frac{2^d}{2\pi} \int_0^{2\pi} \sigma_d(\cos t, \cos 2t, \dots, \cos nt)\, \mathrm{d}t, \ \ d = 0,\dots,n. \tag{10.45}$$

Proof. Recall that by formula (10.38) we have

$$Q_k(n) = \frac{1}{2\pi} \int_0^{2\pi} \prod_{s=1}^{n} (k - 2 + 2\cos st)\, \mathrm{d}t,$$

hence $Q_k(n)$ is a monic polynomial of degree n in $k-2$.

1° By Theorem 10.3, $Q_k(n)$ represents the number of ordered partitions of $[n]$ into k subsets $A_1,\dots,A_k$, with the property $\sigma(A_1) = \sigma(A_k)$.

Consider a 3-partition A,B,C of $[n]$ such that $\sigma(A) = \sigma(C)$ and assume that $A \cup C$ has d elements, $d = 0,\dots,n$ (denote the number of these 3-partitions by $N(d,n)$). The number of ordered partitions of $[n]$ into k subsets generated by this configuration, having the properties $A_1 = A$ and $B = A_2 \cup \cdots \cup A_{k-1}$ and $A_k = C$ is $(k-2)^{n-d}$ (i.e., the number of functions between a set with $n-d$ elements and a set with $k-2$ elements).

Clearly, $Q_k(n)$ is as a linear combination of powers of $k-2$, where the coefficient of $(k-2)^{n-d}$ has the multiplicity $N(d,n)$.

2° For $d = 0,\dots,n$ the coefficients are

$$N(d,n) = \frac{2^d}{2\pi} \int_0^{2\pi} \sum_{1 \le k_1 < k_2 < \cdots < k_d \le n} \cos k_1 t \cos k_2 t \cdots \cos k_d t\, \mathrm{d}t. \quad \square \tag{10.46}$$

Corollary 10.1. *Let $N_{k_1,\dots,k_d}$ be the number of solutions of the 2-signum equation*

$$\pm k_1 \pm k_2 \pm \cdots \pm k_d = 0,$$

(i.e., the number of ordered 2-partitions with equal sums of the set $\{k_1,\dots,k_d\}$). The following relation holds true

$$N(d,n)=\sum_{1\le k_1<k_2<\cdots<k_d\le n} N_{k_1,\dots,k_d}. \tag{10.47}$$

Proof. The following identity is known to hold (see, e.g., [34]):

$$2^d\prod_{s=1}^{d}\cos k_s t=\sum\cos\left(\pm k_1 t\pm k_2 t\pm\cdots\pm k_d t\right), \tag{10.48}$$

where the sum is taken over all the choices of $+$ and $-$.

Also, notice that for an integer $k\in\mathbb{Z}$ one has

$$\frac{1}{2\pi}\int_0^{2\pi}\cos kt\,\mathrm{d}t=\begin{cases}1, & k=0\\ 0, & k\neq 0.\end{cases}$$

For fixed $1\le k_1<k_2<\cdots<k_d\le n$, the integral of (10.46) gives $N_{k_1,\dots,k_d}$, by (10.48). Summing over all such configurations we obtain (10.47). □

We can now easily compute some coefficients.

Case $d=0$. First, one has $N(0,n)=1$.
Case $d=1$. For $k_1=1,\dots,n$, $N_{k_1}=0$, so $N(1,n)=0$ by Corollary 10.1.
Case $d=2$. Whenever $1\le k_1<k_2\le n$ we have $N_{k_1,k_2}=0$, hence $N(2,n)=0$.
Case $d=3$. By Corollary 10.1, $N(3,n)$ corresponds to the number of ordered triplets (k_1,k_2,k_3) such that $1\le k_1<k_2<k_3\le n$ such that $k_1+k_2=k_3$. This is the number of pairs (k_1,k_2) with $1\le k_1<k_2<n$ and $k_1+k_2\le n$.

If $k_1=1$, then k_2 takes the values $2,\dots,n-1$; If $k_1=2$, then k_2 takes the values $3,\dots,n-2$, and so on. Finally, if $k_1=\lfloor\frac{n}{2}\rfloor$ then one has $k_2=\lfloor\frac{n}{2}\rfloor+1$ for n odd, and there is no solution k_2 for n even. This gives the expression

$$N(3,n)=2\left\lfloor\frac{n}{2}\right\rfloor\left(n-\left\lfloor\frac{n}{2}\right\rfloor-1\right)=\left\lfloor\frac{n^2}{2}\right\rfloor,$$

where the last formula is obtained by trying even and odd cases. One may notice that this sequence corresponds to the OEIS entry A007590.

Case $d=n$. One obtains

$$N(n,n)=2^n\cdot\frac{1}{2\pi}\int_0^{2\pi}\prod_{s=1}^{n}\cos st\,\mathrm{d}t=Q_2(n)=N_{1,2,\dots,n}.$$

10.3.5 Conjectures concerning $Q_k(n)$

We conjecture the asymptotic behaviour and some properties of $Q_k(n)$, which relate to the sequence containing perfect powers.

Conjecture 10.4. For $k \geq 2$, the following asymptotic formula holds

$$Q_k(n) \sim \frac{\sqrt{3}}{2} \cdot \frac{1}{\sqrt{\pi}} \cdot \frac{k^{n+\frac{1}{2}}}{n^{3/2}},$$

as $n \to \infty$. The formula for $Q_2(n)$ conjectured by Andrica and Tomescu in 2002 was proved by Sullivan in 2013, while the asymptotic formula for $Q_3(n)$ has been proposed by Finch in 2009 (see A007576 in [211]).

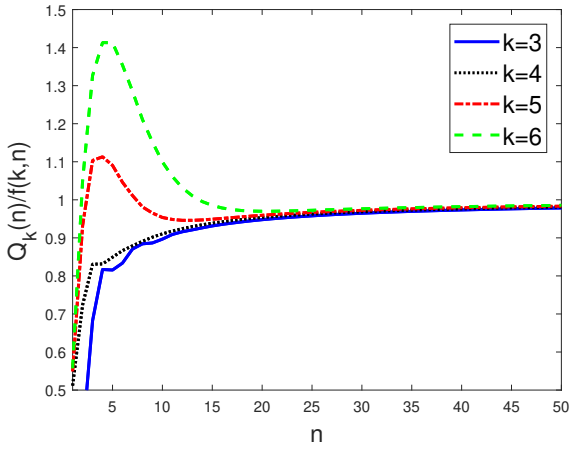

Fig. 10.3 First 50 terms of $\frac{Q_k(n)}{f(k,n)}$ evaluated for $k = 3,4,5,6$, with $f(k,n) = \frac{\sqrt{3}}{2\sqrt{\pi}} \cdot \frac{k^{n+\frac{1}{2}}}{n^{3/2}}$.

Conjecture 10.5. It seems to us that the sequence $Q_k(3)$ (10.44) (A084380 in OEIS [211]) does not contain any perfect squares, i.e., the elliptic equation

$$x^3 + 2 = y^2$$

has no solution in positive integers.

This property is linked to a Catalan-type conjecture related to Pillai's equation $a^x - b^y = n$, with $a > 0, b > 0, x > 1, y > 1$ integers. This states that for any integer n, there are finitely many perfect powers whose difference is n. For $n = 2$, the only solution involving perfect powers smaller than 10^{18} was $2 = 3^3 - 5^2$. The number of such solutions is linked to A076427.

We conjecture that:

1° Sequence $Q_k(4)$ (10.44) does not contain any perfect cubes.
It is easily seen that $[(k-2)^2]^2 < Q_k(4) < [(k-2)^2+1]^2$, hence $Q_k(4)$ does not have perfect squares, i.e., the equation

$$x^4 + 4x + 2 = y^3$$

has no solution in positive integers.

2° Sequence $Q_k(5)$ (10.42) does not contain any perfect fourth powers.
This is to say that the only non-negative integer solution of the equation

$$x^5 + 8x^2 + 6x = y^4$$

is the trivial solution $x = y = 0$.

3° Sequence $Q_k(6)$ (10.43) does not contain any perfect fifth powers.
This is equivalent to the equation

$$x^6 + 12x^3 + 16x^2 + 6x = y^5$$

having no solution in non-negative integers, apart from $x = y = 0$.

The items 1°, 2° and 3° of Conjecture 10.5 have been checked up to $k = 10^4$.

The only perfect power encountered in sequences $Q_k(4)$, $Q_k(5)$ or $Q_k(6)$ was found for $n = 5$ and $k = 8$ where $Q_8(5) = 6^5 + 8 \cdot 6^2 + 6 \cdot 6 = 8100 = 90^2$.

We suggest that for $j \geq 2$, the number of perfect powers x^l in the sequence $Q_k(j+1)$ is zero for $l = j$, and finite for $2 \leq l < j$.

References

1. Albertson, M. O., Hutchinson, J. P., *Discrete Mathematics with Algorithms*, John Wiley & Sons, New York, 1988.
2. Alter, R., Kubota, K. K., *Multiplicities of second order linear recurrences*, Trans. Amer. Math. Soc., **178** (1973), 271–284.
3. André-Jeannin, R., *Summation of reciprocals in certain second-order recurring sequences*, Fibonacci Quart., **35**(1) (1997), 68–74.
4. Andreescu, T., Andrica, D., *360 Problems for Mathematical Contests*, GIL, Zalău, 2003.
5. Andreescu, T., Andrica, D., *Number Theory. Structures, Examples, and Problems*, Birkhäuser Verlag, Boston-Berlin-Basel, 2009.
6. Andreescu, T., Andrica, D., *Complex Numbers from A to . . . Z*, Second Edition, Birkhäuser, Boston, 2014.
7. Andreescu, T., Andrica, D., *Quadratic Diophantine Equations*, Developments in Mathematics, Springer, 2015.
8. Andreescu, T., Zuming, F., *A Path To Combinatorics for Undergraduates: Counting Strategies*, Birkhäuser, 2004.
9. Andreescu, T., Crişan, V., *Mathematical Induction. A Powerful and Elegant Method of Proof*, XYZ Press, 2017.
10. Andrejic, V., *On Fibonacci powers*, Univ. Beograd. Publ. Elektrotehn. Fak. Ser. Mat., **17** (2006), 38–44.
11. Andrews, G. E., *A theorem on reciprocal polynomials with applications to permutations and compositions*, Amer. Math. Monthly, **82** (1975), 830–833.
12. Andrews, G. E., *The Theory of Partitions*, Cambridge University Press, 1998.
13. Andrews, G. E., Eriksson, K., *Integer Partitions*, Cambridge University Press, Second Edition, 2010.
14. Andrica, D., *A combinatorial result concerning the product of two or more derivatives*, Bull. Cal. Math. Soc., **92**(4) (2000), 299–304.
15. Andrica, D., Bagdasar, O., *Some remarks on 3-partitions of multisets*, Electron. Notes Discrete Math., Proceedings of the 2nd IMA TCDM 2018, **70** (2018), 1–8.
16. Andrica, D., Bagdasar, O., *The Cauchy integral formula with applications to polynomials, partitions and sequences*, Proceedings of the XV^{th} International Conference on Mathematics and its Applications, Timişoara, November 1–3, 2018, Editura Politehnica, Timişoara-2019, 12–25.
17. Andrica, D., Bagdasar, O., *On some results concerning the polygonal polynomials*, Carpathian J. Math., **35** (2019), 1–12.
18. Andrica, D., Bagdasar, O., *A new formula for the coefficients of Gaussian polynomials*, An. Şt. Univ. Ovidius Constanţa, **27**(3) (2019), 25–36.
19. Andrica, D., Bagdasar, O., *Remarks on a family of complex polynomials*, Appl. Anal. Discr. Math., **13**(2) (2019), 605–618.

20. Andrica, D., Bagdasar, O., *On cyclotomic polynomial coefficients*, Malays. J. Math. Sci., Proceedings of "Groups, Group Rings, and Related Topics - 2017" (GGRRT 2017), 19 - 22 Nov 2017, Khorfakan, UAE, **14**(3) (2020), 389–402.
21. Andrica, D., Bagdasar, O., *Recurrent Sequences: Key Results, Applications and Problems*, Springer, 2020.
22. Andrica, D., Bagdasar, O., *On k-partitions of multisets with equal sums*, Ramanujan J., **55** (2021), 421–435.
23. D. Andrica, O. Bagdasar, *Remarks on the coefficients of the inverse cyclotomic polynomials*, Mathematics **11**(17) (2023).
24. D. Andrica, O. Bagdasar, *Some remarks on the coefficients of cyclotomic polynomials*. In: J. Guàrdia, N. Minculete, D. Savin, M. Vela, A. Zekhnini (eds.), New Frontiers in Number Theory and Applications, Trends in Mathematics, Birkhäuser, Cham, pp. 29–49, 2024.
25. Andrica, D., Bagdasar, O., Marinescu D.-Şt., *The combinatorial nature of some trigonometric integrals*, Creative Math. Inf., **32**(2) (2023), 1–7.
26. Andrica, D., Bagdasar, O., Ţurcaş, G.-C., *The number of partitions of a set and superelliptic Diophantine equations*, In: Raigorodskii, A. M., Rassias M. Th., (eds) *Discrete Mathematics and Applications. Springer Optimization and Its Applications*. Vol 165, Springer, Cham, pp. 35–55, 2020.
27. Andrica, D., Bagdasar, O., Ţurcaş, G.-C., *On some new results for the generalised Lucas sequences*, An. Şt. Univ. Ovidius Constanţa, **29**(1) (2021), 17–36.
28. Andrica, D., Bagdasar, O., and Ţurcaş, G.-C., *Topics on Discrete Mathematics and Combinatorics*, Cluj University Press, Cluj Napoca, 2023.
29. Andrica, D., Bagdasar, O., Ţurcaş, G.-C., *An integral formula for the coefficients of the inverse cyclotomic polynomial*, An. Şt. Univ. Ovidius Constanţa, **33**(1) (2025), pp. 16. (accepted)
30. Andrica, D., Bagdasar, O., Ţurcaş, G.-C., *Remarks on the coefficients of ternary cyclotomic and inverse cyclotomic polynomials*, Bull. Transilv. Univ. Braşov, Series III: Mathematics and Computer Science, (2025), pp. 16. (to appear)
31. Andrica, D., Buzeţeanu, Ş., *The reduction of a second-order linear recurrence and some consequences*, G.M. perfecţionare metodică şi metodologică în matematică şi informatică, **3-4** (1982), 148–152 (in Romanian).
32. Andrica, D., Buzeţeanu, Ş., *On the reduction of the linear recurrence of order r*, Fibonacci Quart., **21**(1) (1985), 81–84.
33. Andrica, D., Buzeţeanu, Ş., *Relatively dense universal sequences for the class of continuous periodical functions of period T*, Mathematica-L'Analyse Numérique et la Théorie de l'Approximation, **16** (1987), 1–9.
34. Andrica, D., Ionaşcu, E. J., *Some unexpected connections between Analysis and Combinatorics*. In: Rassias Th. M., Pardalos, P., (eds.), *Mathematics Without Boundaries. Topics in Pure Mathematics*, Springer, pp. 1–20, 2014.
35. Andrica, D., Ionaşcu, E. J., *The signum equation for Erdös-Surányi sequences*, INTEGERS, **15A** (2015), 1–9.
36. Andrica, D., Piticari, M., *Problem U23*, Mathematical Reflections, **4** (2006).
37. Andrica, D., Piticari, M., *On some interesting trigonometric sums*, Acta Univ. Apulensis Math. Inform., **15** (2008), 299–308.
38. Andrica, D., Toader, Gh., *On systems of linear recurrences*, Itinerant Seminar on Functional Equations, Approximation and Convexity, "Babeş-Bolyai" University, Cluj-Napoca, **7** (1986), 5–12.
39. Andrica, D., Toader, Gh., *On homographic recurences*, Seminar on Mathematical Analysis, "Babeş-Bolyai" University, Cluj-Napoca, **4** (1986), 55–60.
40. Andrica, D., Tomescu, I., *On an integer sequence related to a product of trigonometric fuctions, and its combinatorial relevance*, J. Integer Seq., **5** (2002), Article 02.2.4.
41. Andrica, D., Văcăreţu, D., *Representation theorems and almost unimodal sequences*, Studia Univ. Babeş-Bolyai, Mathematica, Volume **LI**(4) (2006), 23–33.

42. Apostol, T. M., *Introduction to Analytic Number Theory*, Springer, New York, 1976.
43. Bachman, G., *On the Coefficients of Cyclotomic Polynomials*, Mem. Amer. Math. Soc., Vol. 106, no. 510, 1993.
44. Bagdasar, O., *Concise Computer Mathematics: Tutorials on Theory and Problems*, Springer Briefs in Computer Science, Springer, 2013.
45. Bagdasar, O., *On some functions involving the lcm and gcd of integer tuples*, Appl. Maths. Inform. and Mech., **6**(2) (2014), 91–100.
46. Bagdasar, O., *On the geometry and applications of complex recurrent sequences*, Doctoral Thesis, Babeş-Bolyai University, Cluj Napoca, 2015.
47. Bagdasar, O., Andrica, D., *New results and conjectures on 2-partitions of multisets*, in: Proc. 7th International Conference on Modeling, Simulation, and Applied Optimization (ICMSAO), Sharjah, IEEE Xplore (2017), 1–5.
48. Bagdasar, O., Chen, M., *A Horadam-based Pseudo-random Number Generator*, Proceedings of 16th UKSim, Cambridge (2014), 226–230.
49. Bagdasar, O., Hedderwick, E., Popa I.-L., *On the ratios and geometric boundaries of complex Horadam sequences*, Electron. Notes Discrete Math., Proceedings of TREPAM 2017, **68** (2018), 63–70.
50. Bagdasar, O., Larcombe, P. J., *On the characterization of periodic complex Horadam sequences*, Fibonacci Quart., **51**(1) (2013), 28–37.
51. Bagdasar, O., Larcombe, P. J., *On the number of complex periodic complex Horadam sequences*, Fibonacci Quart., **51**(4) (2013), 339–347.
52. Bagdasar, O., Larcombe, P. J., *On the characterization of periodic generalized Horadam sequences*, J. Differ. Equ. Appl., **20**(7) (2014), 1069–1090.
53. Bagdasar, O., Larcombe, P. J., Anjum, A., *Particular Orbits of Periodic Horadam Sequences*, Octogon Math. Mag., **21**(1) (2013), 87–98.
54. Bagdasar, O., Larcombe, P. J., Anjum, A., *On the structure of periodic complex Horadam sequences*, Carpathian J. Math., **32**(1) (2016), 29–36.
55. Bagdasar, O., Larcombe, P. J., *On the masked periodicity of Horadam sequences: A generator-based approach*, Fibonacci Quart., **55**(4) (2013), 332–339.
56. Bagdasar, O., Popa I.-L., *On the geometry of certain periodic non-homogeneous Horadam sequences*, Electron. Notes Discrete Math., Proceedings of the 1st IMA TCDM 2016, **56** (2016), 7–13.
57. Bastida, J. R., *Quadric Properties of a Linearly Recurrent Sequence*, Proceedings of the Tenth Southeastern Conference on Combinatorics, Graph Theory and Computing, Winnipeg, Canada, Utilitas Math., 1979.
58. Bastida, J. R., DeLeon, M. J., *A Quadratic Property of Certain Linearly Recurrent Sequences*, Fibonacci Quart., **19**(2) (1981), 144–146.
59. Bateman, P. T., *Note on the coefficients of cyclotomic polynomial*, Bull. Amer. Math. Soc., **55**(12) (1949), 1180–1181.
60. Bateman, P. T., Pomerance, C., Vaughan, R. C., *On the coefficients of cyclotomic polynomial*, Coll. Math. Soc. J. Bolyai, Budapest, **34** (1981), 171–202.
61. Bateman, P.T., Hildebrand, A.J, Purdy, G.B., *Sums of distinct squares*, Acta Arithmetica, **LXVII**(4) (1994), 349–380.
62. Beiter, M., *The midterm coefficient of the cyclotomic polynomial* $F_{pq}(x)$, Amer. Math. Monthly., **71**(7) (1964), 769–770.
63. Beiter, M., *Magnitude of the coefficients of the cyclotomic polynomials* $\Phi_{pqr}(X)$, Amer. Math. Monthly, **75**(4) (1968), 370–372.
64. Beiter M., *Magnitude of the coefficients of the cyclotomic polynomials* $\Phi_{pqr}(X)$ *II*, Duke Math. J., **38**(3) (1971), 591–594.
65. Ben-Naim, E., *Mixing of diffusing particles*, Phys. Rev. E, **82** (2010), 061103.
66. Bender, E. A., *Partitions of multisets*, Discrete Math., **9** (1974), 301–311.
67. Bender, E. A., Devitt J. S., Richmond L. S., *Partitions of multisets II*, Discrete Math., **50** (1984), 1–8.
68. Berstel, J., Mignotte, M., *Deux propriétés décidables des suites récurrentes linéaires*, Bull. Soc. Math. France, **104** (1976), 175–184.

69. Berstel, J., Perrin, D., *The origins of combinatorics on words*, European J. Combin., **28** (2007), 996–1022.
70. Bibak, Kh., Shirdareh H., *Some trigonometric identities involving Fibonacci and Lucas Numbers*, J of Int. Seq., **12** (2009), Article 09.8.4.
71. Bilu, Y., Hanrot, G., Voutier, P. M., *Existence of primitive divisors of Lucas and Lehmer numbers*, Journal für die reine und angewandte Mathematik, **2001**(539) (2001), 75–122.
72. Bloom, D. M., *On the coefficients of the cyclotomic polynomials*, Amer. Math. Monthly, **75** (1968), 372–377.
73. Boonklurb, R., Laoharenoo, A., *Exact value of integrals involving product of sine or cosine function*, New Zealand J. Math., **53** (2022), 51–61.
74. Borwein, P., Moser, W. O. J., *A survey of Sylvester's problem and its generalizations*, Aequationes Mathematicae, **40**(1) (1990), 111–135.
75. Borwein, P., *Computational Excursions in Analysis and Number Theory*, CMS Books Math. 10, Springer Verlag, 2002.
76. Borwein, P., Erdélyi, T., *Polynomials and Polynomial Inequalities*, New York, Springer-Verlag, 1995.
77. Branson, D., *Stirling numbers and Bell numbers: their role in combinatorics and probability*, Math. Sci., **25** (2000), 1–31.
78. Brânzei, D., a.o., *Recurrent Sequences in College*, GIL, Zalău, 1996 (in Romanian).
79. Bressoud, D. M., *Unimodality of Gaussian polynomials*, Discrete Math., **99**(1) (1992), 17–24.
80. Brown Jr., J. L., *Note on complete sequences of integers*, Amer. Math. Monthly, **68**(6) (1961), 557–560.
81. Brown Jr., J. L., *Generalization of Richert's theorem*, Amer. Math. Monthly, **83**(8) (1976), 631–634.
82. Bumbăcea, R., *Graphs: An Introduction*, XYZ Press, 2020.
83. Buschman, R. G., *Fibonacci numbers, Chebyshev polynomials generalizations and difference equations*, Fibonacci Quart., **1**(4) (1963), 1–7.
84. Camina, A., Lewis, B., *An Introduction to Enumeration*, Springer, 2011.
85. Carlitz, L., *Generating functions for powers of certain sequences of numbers*, Duke Math. J., **29** (1962), 521–537.
86. Carlitz, L., *Some determinants containing powers of Fibonacci numbers*, Fibonacci Quart., **4**(2) (1966), 129–134.
87. Carlitz, L., *The number of terms in the cyclotomic polynomial* $F_{pq}(x)$, Amer. Math. Monthly, **73**(9) (1966), 979–981.
88. Chen, W. Y. C., Hou, Q-H., *Factors of the Gaussian coefficients*, Discrete Math., **306**(13) (2006), 1446–1449.
89. Carson, T. R., *Periodic recurrence relations and continued fractions*, Fibonacci Quart., **45**(4) (2007), 357–361.
90. Cartan, H., *Elementary Theory of Analytical Functions in One or More Complex Variables*, Hermann, Paris, 1961 (in French).
91. Cassels, J. W. S., *Local fields*, Cambridge University Press, 1986.
92. Cerlienco, L., Mignotte, M., Piras. F., *Linear Recurrent Sequences: (Algebraic and Arithmetic Properties)*, Publ. Inst. Rech. Math. Avancée, 1984 (in French).
93. Cerlienco, L., Piras. F., *Powers of a matrix*, Boll. Un. Mat. Ital., **6**(2B) (1983), 681–690.
94. Clapperton, J. A., Larcombe, P. J., Fennessey, E. J., *On iterated generated functions for integer sequences*, Utilitas Math., **77** (2008), 3–33.
95. Cobzaş, Şt., *Mathematical Analysis (Differential Calculus)*, Cluj University Press, Cluj Napoca, 1997 (in Romanian).
96. Cox, D. A., *Galois Theory*, John Wiley & Sons, Vol. 61, 2011.
97. Crandall, R., Pomerance, C., *Prime Numbers: A Computational Perspective*, Springer, New York, Second Edition, 2005.
98. Cuculescu, I., *A simple proof of a formula of Perron*, An. Univ. "C. I. Parhon" Bucureşti, Mat. Fiz., **25** (1960), 7–8 (in Romanian).

99. Dell'Amico, M., Martello, S., *Reduction of the Three-Partition Problem*, J. Comb. Optim., **3**(1) (1999), 17–30.
100. de Kerf, J., *From Fibonacci to Horadam*, Vector, **15** (1999), 122–130.
101. Deza, M., *On minimal number of terms in representation of natural numbers as a sum of Fibonacci numbers*, Fibonacci Quart., **15**(4) (1977), 237–238.
102. Djukić, D., a.o., *The IMO Compendium. A Collection of Problems Suggested for the International Mathematical Olympiads: 1959–2004*, Springer, 2006.
103. Dresden, G. P., *On the middle coeffcient of a cyclotomic polynomial*, Amer. Math. Monthly, **111**(6) (2004), 531–533.
104. Dressler, R.E., *A stronger Bertrand's postulate with an application to partitions*, Proc. Amer. Math. Soc., **33**(2) (1972), 226-228.
105. Drimbe, M.O., *A problem of representation of integers* (Romanian), G.M.-B, **10-11** (1983), 382-383.
106. Eidswick, J. A., *A Proof of Newton's Power Sum Formulas*, Amer. Math. Monthly, **75**(4) (1968), 396–397.
107. Endo, M., *On the coefficients of the cyclotomic polynomials*, Comment. Math. Univ. St. Pauli., **23** (1974/75), 121–126.
108. Entringer, R. C., *Representation of m as* $\sum_{k=-n}^{n} \epsilon_k k$, Canad. Math. Bull., **11** (1968), 289–293.
109. Erdös, P., *On an elementary proof of some asymptotic formulas in the theory of partitions*, Ann. Math., **43**(2) (1942), 437–450.
110. Erdös, P., *On the coefficients of the cyclotomic polynomial*, Bull. Amer. Math. Soc., **52** (1946), 179–184.
111. Erdös, P., Vaughan, R. C., *Bounds for r-th coefficients of cyclotomic polynomials*, J. London Math. Soc., **8**(2) (1974), 393–400.
112. Everest, G., van der Poorten, A., Shparlinski, I., Ward, T., *Recurrence Sequences*, Mathematical Surveys and Monographs, Vol. 104, American Mathematical Society, Providence, U.S.A., 2003.
113. Fairgrieve, S., Gould, H. W., *Product difference Fibonacci identities of Simson, Gelin-Ces'aro, Tagiuri and generalizations*, Fibonacci Quart., **43**(2) (2005), 137–141.
114. Finch, S. R., *Signum equations and extremal coefficients*, `people.fas.harvard.edu/~sfinch/`.
115. Fredman, M. L., Tarjan, R. E., *Fibonacci heaps and their uses in improved network optimization algorithms*, J. Assoc. Comput. Mach. **34**(3) (1987), 596–615.
116. Garey, M. R., Johnson, D. S., *Complexity results for multiprocessor scheduling under resource constraints*, SIAM J. Comput., **4** (1975), 397–411.
117. Garey, M. R., Johnson, D. S., *Computers and Intractability; A Guide to the Theory of NP-Completeness*, Freeman, San Francisco, 1979.
118. Garnier, N., Ramaré O., *Fibonacci numbers and trigonometric identities*, Fibonacci Quart., **46** (2008), 1–7.
119. Gould, H. W., Quaintance, J., *Products of numbers which obey a Fibonacci-type recurrence*, Fibonacci Quart., **45** (2007), 337–346.
120. Granville, A., *Number Theory Revealed: An Introduction*, American Math. Society, Providence, Rhode Island, 2020.
121. Grytczuk, A., Tropak, B., *A numerical method for the determination of the cyclotomic polynomial coefficients*, In: Pethö, A., Pohst M. E., Williams, H. C., Zimmer, H. G., (eds.), *Computational Number Theory*. Berlin: de Gruyter, pp. 15–19, 1991.
122. Guiaşu, S., *Applications of Information Theory: Dynamical Systems, Cybernetical Systems (Romanian)*, Ed. Acad. R. S. Romania, Bucharest, 1968.
123. Goodman, F. M., de Hope, P., Jones, V. F. R., *Coxeter Graphs and Towers of Algebras*, Springer Verlag, 1989.
124. Graham, I., Kohr, G., *Geometric Function Theory in One and Higher Dimensions*, CRC Press, 2003.

125. Halava, V., Harju, T., Hirvensalo, M., *Positivity of Second Order Linear Recurrent Sequences*, T.U.C.S. Tech. Rep. No. 685, Turku Centre for Computer Science, University of Turku, Finland, 2005.
126. Halton, J., *Some properties associated with square Fibonacci numbers*, Fibonacci Quart., **5**(4) (1967), 347–354.
127. Hardy, G. H., Wright, E. M., *An Introduction to the Theory of Numbers*, Oxford University Press, Oxford, Fifth Edition, 1979.
128. Hardy, G. H., Seshu Aiyar, P. V., Wilson B. M. (eds.), *Collected Papers of Srinivasa Ramanujan*, Cambridge University Press, 2016.
129. Haukkanen, P., *A note on Horadam's sequence*, Fibonacci Quart., **40** (2002), 358–361.
130. He, T.-X., Shiue, P. J.-S., *On sequences of numbers and polynomials defined by linear recurrence relations of order 2*, Int. J. Math. Math. Sci., **2009** (2009), Article 709386.
131. He, X., Lv. J.-B., Zhou, N. H., *Note on the number of ordered k-partitions of multiset $M_d[n]$ with equal sums*, Mediterr. J. Math. **20**, 228 (2023).
132. Hellekalek, P., *Good random number generators are (not so) easy to find*, Math. Comput. Simulation, **46** (1998), 485–505.
133. Hilton, A. J. W., *On the partition of Horadam's generalized sequences into generalized Fibonacci and generalized Lucas sequences*, Fibonacci Quart., **12**(4) (1974), 339–345.
134. Horadam, A. F., *A generalized Fibonacci sequence*, Amer. Math. Month., **68** (1961), 455–459.
135. Horadam, A. F., *Basic properties of a certain generalized sequence of numbers*, Fibonacci Quart., **3**(3) (1965), 161–176.
136. Horadam, A. F., *Generating functions for powers of a certain generalised sequence of numbers*, Duke Math. J., **32** (1965), 437–446.
137. Horadam, A. F., *Special properties of the sequence $w_n(a,b;p,q)$*, Fibonacci Quart., **5**(5) (1967), 424–434.
138. Horadam, A. F., *Tschebyscheff and other functions associated with the sequence $\{w_n(a,b;p,q)\}$*, Fibonacci Quart., **7**(1) (1969), 14–22.
139. Horadam, A. F., *Elliptic functions and Lambert series in the summation of reciprocals in certain recurrence-generated sequences*, Fibonacci Quart., **26**(2) (1988), 98–114.
140. Horadam, A. F., *Associated sequences of general order*, Fibonacci Quart., **31**(2) (1993), 166–172.
141. Horadam, A. F., *A synthesis of certain polynomial sequences*. In: Bergum, G. E., Philippou, A. N. Horadam, A. F. (Eds.), *Applications of Fibonacci numbers*, Vol. 6, Kluwer, Dordrecht, Netherlands, pp. 215–229, 1996.
142. Horadam, A. F., *Extension of a synthesis for a class of polynomial sequences*, Fibonacci Quart., **34**(1) (1996), 68–74.
143. Horadam, A. F., Shannon, A. G., *Generalization of identities of Catalan and others*, Port. Math., **44** (1987), 137–148.
144. Horzum, T., Kocer, E. G., *On some properties of Horadam polynomials*, Int. Math. Forum, **4** (2009), 1243–1252.
145. Hu, H., Sun, Z.-W., Liu, J.-X., *Reciprocal sums of second-order recurrent sequences*, Fibonacci Quart., **39**(3) (2001), 214–220.
146. Ireland, K., Rosen, M. *A Classical Introduction to Modern Number Theory*, Graduate Texts in Mathematics, Springer, 1990.
147. Ivanov, N. V., *Linear Recurrences*, preprint, `http://www.mth.msu.edu/~ivanov/Recurrence.pdf` (2008).
148. Jeffery, T., Pereira, R., *Divisibility Properties of the Fibonacci, Lucas, and Related Sequences*, ISRN Algebra, Hindawi, (2014) Article 750325.
149. Jeske, J. A., *Linear recurrence relations - part i*, Fibonacci Quart., **1**(2) (1963), 69–74.
150. Ji, C. G., Li, W. P., *Values of coefficients of cyclotomic polynomials*, Discrete Math., **308**(23) (2008), 5860–5863.
151. Just, E., *Problem E 2367*, Amer. Math, Monthly, **7** (1972), 772.
152. Kelly, L. M., Moser, W. O. J., *On the number of ordinary lines determined by n points*, Can. J. Math., **10** (1958), 210–219.

153. Kiliç, E., Tan, E., *More general identities involving the terms of* $\{W_n(a,b;p,q)\}$, Ars Comb., **93** (2009), 459–461.
154. Kiliç, E., Tan, E., *On binomial sums for the general second order linear recurrence*, Integers: Elec. J. Comb. Num. Theory, **10** (2010), 801–806.
155. Kiliç, E., Ulutaş, Y. T., Ömür, N., *A formula for the generating functions of powers of Horadam's sequence with two additional parameters*, J. Integer Seq., **14** (2011), Article 11.5.6.
156. Kiliç, E., Stănică, P., *Factorizations and representations of binary polynomial recurrences by matrix methods*, Rocky Mount. J. Math., **41** (2011), 1247–1264.
157. Kirillov, A. N., *Unimodality of generalized Gaussian coefficients*, arXiv preprint hep-th/9212152 (1992).
158. Knopfmacher, A., Tichy, R. F., Wagner, S., Ziegler, V., *Graphs, partitions and Fibonacci numbers*, Discrete Appl. Math., **155** (2007), 1175–1187.
159. Knuth, D. E., *The Art of Computer Programming*, Vol. 1, Boston: Addison Wesley, 1975.
160. Knuth, D. E., *Two Notes on Notation*, Amer. Math. Monthly., **99**(5) (1992), 403–422.
161. Knuth, D. E., *The Art of Computer Programming*, Vol. 3, Addison Wesley, Second Edition, 2003.
162. Knuth, D. E., Wilf, H. S., *The power of a prime that divides a generalized binomial coefficient*, J. Reine Angew. Math. **396** (1989), 212–219.
163. Koshy, T., *Fibonacci and Lucas Numbers with Applications*, John Wiley & Sons, Inc., Hoboken, NJ, USA, 2001.
164. Koshy, T., *Pell and Pell−Lucas Numbers with Applications*, Springer-Verlag, New York, 2014.
165. Kosyak, A., Moree, P., Sofos, E., Zhang, B., *Cyclotomic polynomials with prescribed height and prime number theory*, Mathematika, **67** (2021), 214–234.
166. Lam, T. Y., Leung, K. H., *On the Cyclotomic Polynomial* $\Phi_{pq}(x)$, Amer. Math. Monthly, **103**(7) (1996), 562–564.
167. Lando, S. K., *Lectures on Generating Functions*, Student Mathematical Library, Vol. 23, AMS, 2003.
168. Lang, S., *Algebraic Number Theory*, Graduate Texts in Mathematics, Vol. 110, Springer, 1994.
169. Langlois, A., Stehlé, D., *Worst-case to average-case reductions for module lattices*, Designs, Codes and Cryptography, **75**(3) (2015), 565–599.
170. Laohakosol, V., Kuhapatanakul, K., *Reciprocal sums of generalized second order recurrence sequences*, Fibonacci Quart., **46/47**(4) (2009), 316–325.
171. Larcombe, P. J., Bagdasar, O., Fennessey, E. J., *Horadam sequences: a survey*, Bull. Inst. Combin. Appl., **67** (2013), 49–72.
172. Larcombe, P. J., Bagdasar, O., Fennessey, E. J., *On a result of Bunder involving Horadam sequences: A proof and generalization*, Fibonacci Quart., **51**(2) (2013), 174–176.
173. Larcombe, P. J., Bagdasar, O., Fennessey, E. J., *On a result of bunder involving Horadam sequences: a new proof*, Fibonacci Quart., **52**(2) (2014), 175–177.
174. Larcombe, P. J., Fennessey, E. J., *On cyclicity and density of some Catalan polynomial series*, Bull. Inst. Combin. Appl., **71** (2014), 87–93.
175. Larcombe, P. J., Fennessey, E. J., *On Horadam Sequence Periodicity: A New Approach*, Bull. Inst. Combin. Appl., **73** (2015), 98–120.
176. Larcombe, P. J., Fennessey, E. J., *On the phenomenon of Masked Periodic Horadam Sequences*, Utilitas Math., **96** (2015), 111–123.
177. Latapy, M., Phan, T. H. D., Crespelle, C., Nguyen, T. Q., *Termination of Multipartite Graph Series Arising from Complex Network Modelling*, In: Combinatorial Optimization and Applications, Lecture Notes in Computer Science, **6508** (2010), 1–10.
178. Lee, J. Z, Lee, J. S., *Some properties of the sequence* $\{W_n(a,b;p,q)\}$, Fibonacci Quart., **25**(3) (1987), 268–278 & p.283.
179. Lehmer, E., *On the magnitude of the coefficients of the cyclotomic polynomial*, Bull. Amer. Math. Soc., **42** (1936), 389–392.

180. Lehmer, E., *On the infinitude of Fibonacci pseudoprimes*, Fibonacci Quart., **2**(3) (1964), 229–230.
181. Lehmer, D. H., *Some properties of the cyclotomic polynomial*, J. Math. Anal. Appl., **42**(1) (1966), 105–117.
182. Lenstra, A., *Using cyclotomic polynomials to construct efficient discrete logarithm cryptosystems over finite fields*, Information Security and Privacy – ACISP 1997, Lecture Notes in Comput. Sci. 1270, Springer, Berlin, pp. 126–138, 1997.
183. Lupşa, L., Popovici, N., *Generalized unimodal multicriteria optimization problems*, Rev. Anal. Numer. Theor. Approx., **35** (2006), 65–70.
184. Lyubashevsky, V., Peikert, C., Regev, O., *On Ideal Lattices and Learning with Errors over Rings*, Journal of the ACM, **60**(6), November 2013, Association for Computing Machinery, New York, NY, USA.
185. Maier, H., The coefficients of cyclotomic polynomials. In: Berndt, B. C., Diamond, H. G., Halberstam, H., Hildebrand, A. (eds.), *Analytic Number Theory* (Allerton Park IL, 1989), Progr. Math. **85**, Birkhäuser Boston, pp. 349–366, 1990.
186. Maier, H., *Cyclotomic polynomials with large coefficients*, Acta Arith., **64** (1993), 227–235.
187. Maier, H., *The size of the coefficients of cyclotomic polynomials*, In: *Analytic Number Theory* (Allerton Park IL, 1995), Progr. Math. **139**, Birkhäuser Boston, pp. 633–639, 1996.
188. Maier, H., Rassias, M. Th., Tóth, L., *Recent Progress on Topics of Ramanujan Sums and Cotangent Sums Associated with the Riemann Hypothesis*, Monographs in Number Theory, World Scientific Publishing, 2022.
189. Mansour, T., *A formula for the generating functions of powers of Horadam's sequence*, Australas. J. Combin., **30** (2004), 207–212.
190. Margolius, B. H., *Permutations with Inversion*, J. Integer Seq., **4** (2001), Article 01.2.4.
191. Markouchevitch, A., *Four Courses in Mathematics (Recurrent Sequences)*, Mir, Moscou, 1973 (in French).
192. Martin, G. E., *Counting: The Art of Enumerative Combinatorics*, Springer, 2001.
193. McFarland, R. L., *Problem 6457*, **92**(8) (1985), 599–600.
194. McLaughlin, R., *Sequences—Some Properties by Matrix Methods*, Math. Gaz., **64** (1980), 281–282.
195. Melham, R. S., *Summation of reciprocals which involve products of terms from generalized Fibonacci sequences*, Fibonacci Quart., **38**(4) (2000), 294–298.
196. Melham, R. S., *Summation of reciprocals which involve products of terms from generalized Fibonacci sequences—part ii*, Fibonacci Quart., **39**(3) (2001), 264–267.
197. Melham, R. S., Shannon, A. G., *Some congruence properties of generalized second-order integer sequences*, Fibonacci Quart., **32**(5) (1994), 424–428.
198. Melham, R. S., Shannon, A. G., *A generalization of the Catalan identity and some consequences*, Fibonacci Quart., **33**(1) (1995), 82–84.
199. Melham, R. S., *A Fibonacci identity in the spirit of Simson and Gelin-Cesàro*, Fibonacci Quart., **41**(2) (2003), 142–143.
200. Mező, I., *Several generating functions for second-order recurrence sequences*, J. Integer Seq., **12** (2009), Article 09.3.7.
201. Mitek , J., *Generalization of a theorem of Erdős and Surányi*, Comment. Math. Prace Mat., **21** (1980), 173–175.
202. Mitrinovic, D. S., Sándor, J., Crstici, B., *Handbook of Number Theory*, Kluwer, Dordrecht, Netherlands, 1995.
203. Morgado, J., *Note on some results of A.F. Horadam and A.G. Shannon concerning a Catalan's identity on Fibonacci numbers*, Port. Math., **44** (1987), 243–252.
204. Moree, P., *Inverse cyclotomic polynomials*, J. Number Theory, **129** (2009), 667–680.
205. Moritz, R. H., Williams, R. C., *A Coin-Tossing Problem and Some Related Combinatorics*, Math. Mag., **61** (1988), 24–29.
206. Muntean, I., Popa, D., *The Method of Recurrent Sequences*, GIL, Zalău, 1995 (in Romanian).
207. Nagarajan, D., Rameshkumar, A., *Cyclotomic and inverse cyclotomic polynomial*, Adv. Math. Sci. J, **11** (2022), 415–432.

208. Newell, A. C., Pennybacker, M., *Fibonacci patterns: common or rare?*, Procedia IUTAM, **9** (2013), 86–109.
209. Newman, D. J., *Simple analytic proof of the prime number theorem*, Amer. Math. Monthly, **87** (1980), 693–696.
210. Noonea, C. J., Torrilhonb, M., Mitsosa, A., *Heliostat field optimization: A new computationally efficient model and biomimetic layout*, Solar Energy, **86**(2) (2012), 792–803.
211. The On-Line Encyclopedia of Integer Sequences, `https://oeis.org`, OEIS Foundation Inc., 2024.
212. O'Hara, K. M., *Unimodality of Gaussian coefficients: a constructive proof*, J. Comb. Theory A, **53**(1) (1990), 29–52.
213. Oohama, Y., *Performance analysis of the internal algorithm for random number generation based on number systems*, IEEE Trans. Inform. Theory, **57**(3) (2011), 1177–1185.
214. Ouaknine, J., Worrell, J., *Ultimate Positivity is decidable for simple linear recurrence sequences*, CoRR, abs/1309.1914 (2013).
215. Ouaknine, J., Worrell, J., *On the Positivity Problem for simple linear recurrence sequences*, Proc. of ICALP'14. CoRR, abs/1309.1550 (2014).
216. Ouaknine, J., Worrell, J., *Positivity problems for low-order linear recurrence sequences*, Proc. SODA'14. ACM-SIAM (2014).
217. Pak, I., *Partition bijections, a survey*, Ramanujan J., **12** (2006), 5–75.
218. Panneton, F., L'Ecuyer, P., Matsumoto, M., *Improved long-period generators based on linear reccurences modulo 2*, ACM Trans. Math. Software, **32** (2006), 1–16.
219. Prudyus, I., Sumyk, M., *Multiphase signals based on recurrent sequences of maximal length*, Modern Problems of Radio Engineering, Telecommunications and Computer Science (2004), 360–362.
220. Raab, J. A., *A generalization of the connection between the Fibonacci sequence and Pascal's triangle*, Fibonacci Quart., **1**(3) (1963), 21–31.
221. Rabinowitz, S., *Algorithmic manipulation of second-order linear recurrences*, Fibonacci Quart., **37**(2) (1999), 162–177.
222. Ramanujan, S., *A proof of Bertrand's postulate*, J. Indian Math. Soc., **11** (1919), 181–182.
223. Ratsaby, J., *Estimate of the number of restricted integer-partitions*, Appl. Anal. Discrete Math., **2** (2008), 222–233.
224. Reiter, C. A., *Exact Horadam numbers with a Chebyshevish accent*, Vector, **16** (1999), 122–131.
225. Robinson, D. W., *The rank and period of a linear recurrent sequence over a ring*, Fibonacci Quart., **14**(3) (1976), 210–214.
226. Rosen, K. H., *Discrete Mathematics and Its Applications*, 7th ed., McGraw-Hill Education, 2011.
227. Rotkiewicz, A., *Lucas and Frobenius pseudoprimes*, Ann. Math. Sil., **17** (2003), 17–39.
228. Roy, S., *What's the Next Fibonacci Number?*, Math. Gaz., **64**(425) (1980), 189–190.
229. Sándor, J., Crstici, B., *Handbook of Number Theory II*, Springer Science & Business Media, 2004.
230. Sanna, C., *A survey on coefficients of cyclotomic polynomials*, Expositiones Mathematicae, **40**(3) (2022), 469–494.
231. Santana, S. F., Diaz-Barrero, J. L., *Some properties of sums involving Pell numbers*, Miss. J. Math. Sci., **18**(1) (2006), 33–40.
232. Sasu, B., Sasu, S. L., *Discrete Dynamical Systems*, Editura Politehnică, Timişoara, 2013 (in Romanian).
233. Schwarz, W., Spilker, J., *Arithmetical Functions. An introduction to elementary and analytic properties of arithmetic functions and to some of their almost-periodic properties*, London Mathematical Society Lecture Note Series, Vol. 184, Cambridge University Press, 1994.
234. Shannon, A. G., *Generalized Fibonacci numbers as elements of ideals*, Fibonacci Quart., **17**(4) (1979), 347–349.
235. Shannon, A. G., *A generalization of Hilton's partition of Horadam's sequences*, Fibonacci Quart., **17**(4) (1979), 349–357.

236. Shannon, A. G., Horadam, A. F., *Some properties of third-order recurrence relations*, Fibonacci Quart., **10**(2) (1972), 135–145.
237. Shannon, A. G., Horadam, A. F., *Special recurrence relations associated with the sequence* $\{w_n(a,b;p,q)\}$, Fibonacci Quart., **17**(4) (1979), 294–299.
238. Silvester, J. R., *Fibonacci properties by matrix methods*, Math. Gaz., **63**(425) (1979), 188–191.
239. Sitaramachandra, R. R., Suryanabayana, D., *The number of pairs of integers with L.C.M.* $\leq x$, Arch. Math., **21** (1970), 490–497.
240. Soberón, P., *Problem-Solving ethods in Combinatorics. An Approach to Olympiad Problems*, Birkhäuser, 2013.
241. Sprague, R., *Über Zerlegungen in ungleiche Quadratzahlen*, Math. Z., **51** (1948), 289–290.
242. Stănică, P., *Generating functions, weighted and non-weighted sums for powers of second-order recurrence sequences*, Fibonacci Quart., **41**(4) (2003), 321–333.
243. Stanley, R. P., *Weyl groups, the hard Lefschetz theorem and the Sperner property*, SIAM J. Alg. Discr. Meth., **1** (1980), 168–184.
244. Stanley, R. P., *Log-concave and unimodal sequences in algebra, combinatorics, and geometry*, Ann. NY Acad. Sci., **576** (1989), 500–535.
245. Sullivan, B. D., *On a conjecture of Andrica and Tomescu*, J. Integer Seq., **16** (2013), Article 13.3.1.
246. Suzuki, J., *On coefficients of cyclotomic polynomials*, Proc. Japan Acad. Ser. A Math. Sci., **63** (1987), 279–280.
247. Tani, N. B., Bouroubi, S., *Enumeration of the partitions of an integer into parts of a specified number of different sizes and especially two sizes*, J. Integer Seq., **14** (2011), Article 11.3.6.
248. Tetiva, M., *A representation problem*, Recreaţii Matematice, **2** (2010), 123–127 (in Romanian).
249. Tetiva, M., *A representation theorem II* Recreaţii Matematice, **1** (2012), 5–10 (in Romanian).
250. Thangadurai, R., *On the Coefficients of Cyclotomic Polynomials*. In: Proceedings of the Summer School on Cyclotomic Fields, June 1999.
251. Toader, Gh., *Generalized double sequences*, Rev. Anal. Numér. Théor. Approx., **16** (1987a), 81–85.
252. Tucker, A., *Applied Combinatorics*, 6th ed., Wiley, 2012.
253. Udrea, G., *A note on the sequence* $(W_n)_{n\geq 0}$ *of A.F. Horadam*, Port. Math., **53** (1996), 143–155.
254. Vălcan, D., Bagdasar, O., *Generalizations of some divisibility relations in* $\mathbb{N}$, Creative Math. & Inf., **18**(1) (2009), 92–99.
255. Vaughan, R. C., *Bounds for the coefficients of cyclotomic polynomials*, Michigan Math. J., **21** (1975), 289–295.
256. Vince, A., *Period of a linear recurrence*, Acta Arith., **39** (1981), 303–311.
257. Vogel, H., *A better way to construct the sunflower head*, Mathem. Biosci., **44** (1979), 179–189.
258. Vorobiev, N. N., *Fibonacci Numbers*, Birkhäuser Verlag, Basel-Boston, 2002.
259. Weyl, H., *Über die gleichverteilung von zahlen mod. eins*, Math. Ann., **77**(3) (1916), 313–352 (in German).
260. Wilf, H., *Generatingfunctionology*, Academic Press, New York, 1994.
261. Wright, E. M., *The representation of a number as a sum of five or more squares*, Quart. J. Math. Oxford, **4** (1933), 37–51.
262. Wunsch, D. A., *Complex Variables with Applications*, Pearson, Third Edition, 2004.
263. Yang, W. C., *Derivatives are essentially integer partitions*, Discrete Math., **222** (2000), 235–245.
264. Yazlik, Y., Taskara, N., *A note on generalized k-Horadam sequence*, Comp. Math. Appl., **63** (2012), 36–41.
265. Zeenath, A. U., Lakshmy, K. V., Cusick, T. W., Sethumadhavan, M., *Construction and enumeration of balanced rotation symmetric Boolean functions*, Discrete Appl. Math., **357** (2024), 197–208.

266. Zeilberger, D., *A combinatorial proof of Newton's identities*, Discrete Math., **49** (1984), 319.
267. Zeitlin, D., *Generating functions for products of recursive sequences*, Trans. Amer. Math. Soc., **116** (1965), 300–315.
268. Zeitlin, D., *Power identities for sequences defined by* $W_{n+2} = dW_{n+1} - cW_n$, Fibonacci Quart., **3**(4) (1965), 241–256.
269. Zeitlin, D., *On determinants whose elements are products of recursive sequences*, Fibonacci Quart., **8**(4) (1970), 350–359.
270. Zeitlin, D., *General identities for recurrent sequences of order two*, Fibonacci Quart., **9**(4) (1971), 357–388.
271. Zenkevich, I. G., *Application of recurrent relations in chemistry*, J. Chemometrics, **24** (2010), 158–167.
272. Zhang, W., *Some identities involving the Fibonacci numbers*, Fibonacci Quart., **35**(3) (1997), 225–229.
273. Zhang, Z., *Some identities involving generalized second-order integer sequences*, Fibonacci Quart., **35**(3) (1997), 265–268.
274. Zhang, Z., Liu, M., *Generalizations of some identities involving generalized second-order integer sequences*, Fibonacci Quart., **36**(4) (1998), 327–328.

Index

The second edition of this book incorporates significant new results in discrete mathematics and combinatorics. Expanded with additional problems inspired by teaching at Babeș-Bolyai University, enriched examples on the pigeonhole principle and mathematical induction, and a new section on Erdős-Surányi sequences, this revised edition continues to present modern developments in the field, illustrated by numerous examples and applications, while encouraging further research.

UNIVERSITAS CLAUDIOPOLITANA
ROMANIA
PRESA UNIVERSITARĂ

ISBN: 978-606-37-2482-4