Topics in Number Theory and Combinatorics

By

Robert Scherer
DISSERTATION

Submitted in partial satisfaction of the requirements for the degree of

DOCTOR OF PHILOSOPHY

in

MATHEMATICS

in the

OFFICE OF GRADUATE STUDIES

of the

UNIVERSITY OF CALIFORNIA

DAVIS

Approved:

Professor Dan Romik (Chair)

Professor Elena Fuchs

Professor Martin Luu

Committee in Charge

2021

Contents

Abstract

This dissertation consists of four distinct research projects in combinatorics and number theory. The first project, in **Chapter** 2, deals with the Taylor coefficients of a classical modular form, the Jacobi theta constant $\theta_3(\tau) = \sum_{n\in\mathbb{Z}} e^{2\pi i n\tau}$. In particular, we prove a conjecture from [**Rom20**] about periodic congruence behavior of the Taylor coefficients of $\theta_3(\tau)$ around the complex multiplication point $\tau = i/2$. In the process we analyze an interesting two-dimensional fractal pattern, and we prove a new result about the divisibility of the number of set partitions of a certain type.

The second project, in **Chapter** 3, addresses another classical modular form – the weight-two Eisenstein series G_2 – and the closely related Weierstrass $\wp$-function. The chapter can also be viewed as an extended example in the theory of summation of series. G_2 is the quintessential "quasimodular form," as it satisfies a unique transformation property that derives from the conditional convergence of its defining summation, for which there are two standard regularizations that differ by a well-known "error" term. The presence of this error term is fundamental to many further developments in the theory of modular forms. We consider a general class of alternative regularizations of the defining summation, and we furnish an explicit formula for the error term that arises from each member in the class. This error term generalizes the usual one. The Weierstrass $\wp$-function is similarly defined by a standard regularization of conditionally convergent summation over points in a lattice in $\mathbb{C}$, and we describe the error terms arising from alternative summations of $\wp$.

The third project, in **Chapter** 4, is in the area of asymptotic combinatorics. We prove a conjectured asymptotic formula of Kuperberg from the representation theory of the exceptional simple Lie algebra G_2. (Here, G_2 is unrelated to the weight-2 Eisenstein series mentioned in the previous paragraph, but we will use the symbol G_2 in both Chapters 3 and 4 since the notation is standard in both contexts and since the chapters are disjoint.) Given a non-negative sequence $(a_n)_{n\geq 1}$, the identity $B(x) = A(xB(x))$ for generating functions $A(x) = 1 + \sum_{n\geq 1} a_n x^n$ and $B(x) = 1 + \sum_{n\geq 1} b_n x^n$ determines the number b_n of rooted planar trees with $n+1$ vertices such that each vertex having i children can have one of a_i distinct colors. Kuperberg proved in [**Kup96**] that this identity holds in the case that $b_n = \dim \mathrm{Inv}_{G_2}(V(\lambda_1)^{\otimes n})$, where $V(\lambda_1)$ is the 7-dimensional fundamental representation of G_2, and a_n is the number of triangulations of a regular n-gon such that each internal

vertex has degree at least 6. He also observed that $\limsup_{n\to\infty} \sqrt[n]{a_n} \le 7/B(1/7)$ and conjectured that this estimate is sharp, or, in terms of power series, that the radius of convergence of $A(x)$ is exactly $B(1/7)/7$. We prove this conjecture by introducing a new criterion for sharpness in the analogous estimate for general power series $A(x)$ and $B(x)$ satisfying $B(x) = A(xB(x))$. Moreover we significantly refine the conjecture by deriving an asymptotic formula for the sequence $(a_n)_{n\ge 1}$.

The fourth project, in **Chapter** 5, is in the area of discrete probabilistic number theory. We take a new look at the Syracuse map $f : \mathbb{N}_{\text{odd}} \to \mathbb{N}_{\text{odd}}$, defined by $f(x) = (3x+1)/2^{\text{val}_2(3x+1)}$. We prove explicit formulas for the expectation of the sum of binary digits in the values of the first and second iterates of the Syracuse map applied to a random odd integer.

Acknowledgments

The author would like to say a special thank-you to his advisor, Dan Romik, for teaching him about mathematics, and many other important things in life. For introducing him to interesting problems. For believing in him. For pushing him to excel and for his encouragement, patience, and expertise. And generally for all of his help on projects and advising on manuscripts. It has been a privilege to work under his mentorship.

The author would like to thank Greg Kuperberg, for his encouragement, for many helpful conversations, and for the blessing to work on his old problem. The author would also like to thank Michael Drmota for some critical tips about asymptotic analysis.

The author would like to thank his thesis committee, for reading this document.

The author would like to thank the first-floor administration – Tina, Sarah, and Victoria.

The author would like to thank Hamilton S., for his friendship.

The author would like to thank his parents, for their support.

And finally, the author thanks his dearest friend P, for her existence and and her uniqueness, and for breathing life into life.

CHAPTER 1

Introduction

This dissertation consists of four parts, each an individual research project, representing the following fields: Chapters 2 and 3 deal with the theory of Modular Forms, Chapter 4 presents an application from Analytic Combinatorics to a problem in Asymptotic Representation Theory, and Chapter 5 discusses a problem in Discrete Probablistic Number Theory.

Chapter 2 is based on the paper *Congruences modulo primes of the Romik sequence related to the Taylor coefficients of the Jacobi theta constant* θ_3 [**Sch21**]. We prove arithmetical facts about certain partition numbers, and in turn, statements about periodic congruences of the Taylor coefficients of the classical modular form θ_3. **Chapter** 3 is based on the paper *Alternative summation orders for the Eisenstein series* G_2 *and Weierstrass* $\wp$*-function* [**RS20**]. We give an explicit way to evaluate new regularizations of the classical double summations that define G_2 and $\wp$. **Chapter** 4 is based on the paper *A criterion for sharpness in tree enumeration and the asymptotic number of triangulations in Kuperberg's* G_2 *spider* [**Sch20**]. We develop a new criterion for equality in an estimate that is universal in a certain class of tree structures from graph theory. This criterion in turn yields an estimate for the asymptotic growth rate of an important sequence from representation theory. Refinements of this asymptotic estimate are subsequently given by way of singularity analysis. **Chapter** 5 is based on ongoing work with Dan Romik. We derive exact formulas for the expected value of the sum of binary digits in values of the iterated Syracuse map. The chapters are independent and can be read in any order.

In this introductory chapter we provide some preliminary information and describe the main results that will follow. *A comment on notation*: In Chapter 3 the symbol G_2 will be used to denote the weight-2 Eisenstein series. In Chapter 4 the same symbol will be used to denote the exceptional simple Lie Algebra G_2. As these chapters are disjoint, there should not be much risk of confusion in keeping this standard notation.

1.1. Modular forms, Eisenstein series, the Jacobi theta constant, and the Weierstrass $\wp$-function

In this section we aim to give appropriate background context to motivate the results presented in the sequel. For a broad overview of modular forms and their applications, we recommend the books of Zagier [**Zag08**], [**Zag89**]. For a modern algebraic introduction, culminating with the Modularity Theorem, one should see [**DS16**]. For a treatment of half-integer weight modular forms in particular, one may consult the textbook [**Kob93**] as well as the fundamental paper of Shimura [**Shi73**], which pioneered much of the theory. Theta functions and their applications specifically are discussed in detail in [**Bel61**] from a more classical perspective. In addition to these general references, which contain the standard facts that we now describe, further citations of more specialized results will be given below when appropriate.

Loosely speaking, a modular form is a holomorphic function defined on the upper half-plane $\mathbb{H}$ that is nearly-invariant under precomposition with elements of discrete subgroups of the geometry-preserving automorphisms of $\mathbb{H}$, i.e. subgroups of $\mathrm{SL}(2, \mathbb{R})$. More precisely we have the following definition.

Definition 1.1.1. A *holomorphic modular form of weight k*, for $k \in \mathbb{Z}$, is a holomorphic function on the upper half-plane $\mathbb{H}$, satisfying the following properties:

(1) $f(\frac{az+b}{cz+d}) = (cz+d)^k f(z)$ for all $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma := \mathrm{SL}(2, \mathbb{Z})\,,$

(2) $|f(z)|$ is bounded as $\mathrm{Im}(z) \to \infty$.

Often one refers to such an object simply as a "modular form." A few preliminary facts are that the space $M_k(\Gamma)$ of modular forms of a given weight k is finite dimensional, that the graded algebra $M_*(\Gamma) = \bigoplus_{k \geq 4} M_k(\Gamma)$ is isomorphic to the bivariate polynomial algebra over $\mathbb{C}$, and that every modular form f has a Fourier expansion

$$f(\tau) = \sum_{n=0}^{\infty} a_n e^{2\pi i n \tau}.$$

Furthermore, since Γ is generated by the matrices $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, corresponding to the translation $\tau \mapsto \tau + 1$ and the involution $\tau \mapsto -1/\tau$, respectively, to check that f satisfies the first condition above it suffices merely to check with respect to these two maps. A modular form of weight 0 is called a *modular function*, and is truly Γ-invariant. A standard fact is that no holomorphic modular functions exist – one must allow for meromorphic behavior on $\mathbb{H}$ or at ∞. We will give an example below.

One can also consider modular forms with respect to a *subgroup* of Γ, and one can consider *half-integer weights* and further generalizations involving multiplying the factor $(cz + d)^k$ in Definition 1.1.1 (the so-called "automorphy factor") by a Dirichlet character. The precise and cumbersome definition of a half-integer weight form is not universal, and also much more than we need, so we merely illustrate with a classic example that will be important in Chapter 2.

DEFINITION 1.1.2. The *Jacobi theta constant* θ_3 is the function defined on $\mathbb{H}$ by

$$\theta_3(\tau) = 1 + 2\sum_{n=1}^{\infty} e^{2\pi i n^2 \tau} .$$

θ_3 satisfies the periodicity property $\theta_3(\tau + 1) = \theta_3(\tau)$, as well as the modular property

$$\theta_3\left(-\frac{1}{4\tau}\right) = \sqrt{\frac{2\tau}{i}}\,\theta_3(\tau) ,$$

with the square root defined in terms of the principal logarithm. The modular property is a consequence of Poisson summation applied to the Gaussian $x \mapsto e^{-\pi t x^2}$ $(t \in \mathbb{R}^+)$. Taken together, these facts imply that θ_3 is a "modular form of weight 1/2 on the congruence subgroup $\Gamma_0(4)$," where

$$\Gamma_0(4) = \left\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 4 & 1 \end{pmatrix} \right\rangle$$

consists of those elements in Γ for which $c \equiv 0 \pmod 4$. This means that for any $\gamma \in \Gamma_0(4)$, we have

$$\theta_3(\gamma\tau) = \left(\frac{c}{d}\right) \epsilon_d \sqrt{c\tau + d}\,\theta_3(\tau),$$

where $\gamma\tau = \frac{a\tau+b}{c\tau+d}$, $\left(\frac{c}{d}\right)$ is the Kronecker symbol, and ϵ_d takes the value 1 when $d \equiv 1 \pmod 4$ and $-i$ when $d \equiv 3 \pmod 4$. In general, for modularity on a congruence subgroup the bounded-at-infinity condition for the full modular group Γ should be supplemented with the condition that the Fourier coefficients (a_n) are uniformly bounded by a polynomial as $n \to \infty$.

Returning to the setting of the full modular group Γ, we recall the following fundamental family of examples.

Definition 1.1.3. Let $k \geq 4$ be an even integer. The *Eisenstein series of weight* k, denoted G_k, is defined for $\tau \in \mathbb{H}$ by

$$G_k(\tau) = \sum_{m,n} \frac{1}{(n + m\tau)^k}\,, \tag{1.1}$$

with the convention that the summation excludes the index $(m, n) = (0, 0)$, where the summand is undefined. The sum is absolutely and locally uniformly convergent, so that the order of summation is immaterial, and it defines an analytic function on $\mathbb{H}$. The sum is visibly 1-periodic, and upon changing the variable $\tau \mapsto -1/\tau$, one easily finds that $G_k(-1/\tau) = \tau^k G_k(\tau)$. In other words, G_k is a weight-k modular form on Γ. The Fourier expansion is given by

$$G_k(\tau) = 2\zeta(k) + \frac{2(-1)^{k/2}(2\pi)^k}{(k-1)!} \sum_{n=1}^{\infty} \sigma_{k-1}(n) e^{2\pi i n\tau}\,, \tag{1.2}$$

where ζ is the Reimann zeta function and $\sigma_m(n)$ denotes the sum of the m-th powers of the positive divisors of n. In particular, $G_k(\infty) = 2\zeta(k)$.

We can now state concretely the isomorphism mentioned above between $\mathbb{C}[x, y]$ and $M_*(\Gamma)$, namely by identifying x with G_2 and y with G_4. For an example of a modular function, consider the famous *j-invariant*, which has many useful properties – the most famous of which perhaps being the parameterization by its values of the isomorphism classes of elliptic curves over $\mathbb{C}$ – and is defined on $\mathbb{H}$ by

$$j = \frac{1728E_4^3}{E_4^3 - E_6^2},$$

where $E_k := G_k/G_k(\infty)$ for $k \geq 4$. The denominator $\Delta := (E_4^3 - E_6^2)/1728$, called the *modular discriminant*, is a modular form of weight 12 that vanishes at ∞, so that j has a pole.

Since $M_*(\Gamma) = \mathbb{C}[G_4, G_6]$, it is clear that no modular forms of odd weight exists for Γ, and in fact the transformation property in Definition 1.1.1 shows directly that $G_k = 0$ for $k \geq 3$, while for $k = 1$ the sum diverges regardless of whether summation is first done over n or m. But what about the case $k = 2$? Then (1.1) converges, but only *conditionally*, i.e. the value attained is sensitive to the order of summation.

Definition 1.1.4. The *weight-2 Eisenstein series* G_2 is the holomorphic function on $\mathbb{H}$ defined by

$$G_2(\tau) = \sum_m \left[\sum_n \frac{1}{(n+m\tau)^2} \right], \tag{1.3}$$

summed in the indicated order over all $m, n \in \mathbb{Z}$ except for $(m,n) = (0,0)$, where the summand is undefined.

Even for $k = 2$, this regularization of (1.1) can be expanded in a Fourier series by the same method that leads to (1.2), and thus defines a holomorphic function on $\mathbb{H}$. However, switching the order of summation in the defining double sum (1.3) changes its value. Precisely, we have

$$\sum_n \left[\sum_m \frac{1}{(n+m\tau)^2} \right] = \sum_m \left[\sum_n \frac{1}{(n+m\tau)^2} \right] - \frac{2\pi i}{\tau} \tag{1.4}$$

(with both series excluding $(m,n) = (0,0)$ as above). In other words, the discrepancy between the two summation schemes is given by the "residual term" $-2\pi i/\tau$.

Evaluating $G_2(-1/\tau)$ in (1.3) and manipulating the double sum, one finds that (1.4) is equivalent to the *quasimodularity identity*

$$\tau^{-2} G_2(-1/\tau) = G_2(\tau) - \frac{2\pi i}{\tau}. \tag{1.5}$$

One way to prove the validity of (1.5) is to define a modification of G_2, namely

$$G_2^*(\tau) := G_2(\tau) - \pi/\mathrm{Im}(\tau)\,.$$

Then, a somewhat tricky calculation is to show that $G_2^*(\tau) = \lim_{\epsilon\to 0} G_{2,\epsilon}(\tau)$, where

$$G_{2,\epsilon}(\tau) := \sum_{(m,n)\in\mathbb{Z}^2\setminus(0,0)} \frac{1}{(m\tau+n)^2 |m\tau+n|^\epsilon}\,.$$

If we assume this fact, then since $G_{2,\epsilon}$ transforms like a modular form of weight $2+\epsilon$, by the absolute convergence of the sum (resulting from the extra factor of $|m\tau+n|^\epsilon$), one verifies by passing to the limit that $G_2^*(-1/\tau) = \tau^2 G_2^*(\tau)$, and from this (1.5) follows [**Zag08**, p.19].

There is another approach that relies on first *adding* (not multiplying) a corrective term to the summands in (1.3) to again obtain absolute convergence of the sum, and then exploiting the fact that the corrective term is conditionally convergent when summed by itself [**DS16**, p.23]. This trick will be explained in Chapter 3, as it is the fundamental method by which we determine the residual terms that arise from a large class of alternative summations – see the introduction to Chapter 3 in Section 1.3.

If it were not for the residual term $-2\pi i/\tau$ in (1.4) and (1.5), then G_2 would be a weight-2 modular form on Γ. Far from being a deficiency, the presence of this residual term is actually fundamental to the entire theory of modular forms and to many applications in other areas of mathematics. For example, the modular discriminant Δ that we introduced above can alternatively be defined by the identity

$$\frac{d}{dz}\log\Delta(z) = 2\pi i E_2(z)$$

and the boundary condition $\Delta(\infty) = 0$, where $E_2(z) = G_2(z)/G_2(\infty)$ is a normalized version of G_2, whose constant term in the Fourier expansion is 1.

For an application to number theory, consider that equation (1.4) implies that the function $G_{2,N}$ defined on $\mathbb{H}$ by

$$G_{2,N}(\tau) := G_2(\tau) - NG_2(N\tau)$$

is an element of $M_2(\Gamma_0(N))$, the space of modular forms of weight 2 for $\Gamma_0(N)$ (defined like $\Gamma_0(4)$ but with $c \equiv 0 \pmod{N}$). Since $G_{2,2}, G_{2,4}$, and θ_3^4 are all elements of $M_2(\Gamma_0(4))$, which is a 2-dimensional vector space, the linear dependence between them can be determined by comparing the first two terms of their Fourier expansions. Upon so doing one finds that

$$\theta_3(\tau)^4 = -G_{2,4}(\tau)/\pi\,.$$

The nth Fourier coefficient of θ_3^4 is the number of compositions of n^2 as a sum of 4 squares, and the latter identity implies that this number is $8\sigma_1(n)$, which is a result of Jacobi from the 19th century. See [**DS16**, Ch. 1.2] or [**SS03**, Ch. 10].

A recent and spectacular role for the identity (1.4) was played in the solution to the sphere-packing problem in 8 dimensions [**Via17**], where it was used to construct a particularly special eigenfunction of the Fourier transform. The theta constant θ_3 (as well as other Jacobi theta constants) are also involved in that construction (see also [**Coh17**]).

Finally, we recall the Weierstrass $\wp$-function.

Definition 1.1.5. The *Weierstrass $\wp$-function* is the function of two complex variables τ, z (with the dependence on τ usually suppressed in the notation) defined as

$$\wp(z) := \frac{1}{z^2} + \sum_{(m,n)\in\mathbb{Z}^2\setminus\{(0,0)\}} \left[\frac{1}{(z+n+m\tau)^2} - \frac{1}{(n+m\tau)^2}\right], \tag{1.6}$$

for $\tau \in \mathbb{H}$ and $z \notin \mathbb{Z}\tau + \mathbb{Z}$.

The sum is absolutely convergent, precisely because of the "normalization term" $\frac{1}{(n+m\tau)^2}$. Indeed, the $\wp$-function is a fundamental object in the theory of elliptic functions, and the basic idea underlying its definition (1.6) is to try to construct a doubly-periodic function with the two periods $1, \tau$ by summing copies of a single term (for which the best choice turns out to be the meromorphic function z^{-2}, which has a pole of order 2 at the origin) translated over the lattice $\mathbb{Z}\tau + \mathbb{Z}$. This results in the series $\sum_{m,n} \frac{1}{(z+n+m\tau)^2}$, which however is only conditionally convergent. In fact, as we show below in Proposition 3.1.1, switching the order of summation leads to exactly the same "residual term" as for G_2:

$$\sum_m \left[\sum_n \frac{1}{(z+n+m\tau)^2}\right] = \sum_n \left[\sum_m \frac{1}{(z+n+m\tau)^2}\right] + \frac{2\pi i}{\tau}.$$

On the other hand, subtracting $\frac{1}{(n+m\tau)^2}$ from the summands in (1.6) turns the series into an absolutely convergent one, and conveniently still ends up producing a doubly-periodic function. We'll have more to say about this in Section 1.3.2 of the Introduction and in Chapter 3.

The $\wp$-function is a fascinating construction with a natural kinship to modular forms. For one thing, the Laurent expansion of $\wp$ near $z = 0$ is given by

$$\wp(z) = \frac{1}{z^2} + \sum_{n=1}^{\infty}(2n+1)G_{2n+2}(\tau)z^n\,,$$

where $G_m(\tau)$ refers to the weight-m Eisenstein series defined above. Even more excitingly, for fixed $\tau \in \mathbb{H}$ we see that as (1.6) is indexed by points in the lattice $L = \mathbb{Z}\tau + \mathbb{Z}$, we can think of $\wp$ as a function on the torus $\mathbb{C} \setminus L$. It is a remarkable fact that $\wp$ can be used to biject the torus to an elliptic curve in a way that preserves the group structure of the torus. Specifically, it can be shown that the pairs $(y, x) = (\wp'(z), \wp(z))$ $(z \in \mathbb{C} \setminus L)$ biject to solutions of the equation

$$y^2 = 4x^3 - g_2(\tau)x - g_3(\tau),$$

where $g_2 = 60G_4$ and $g_3 = 140G_6$. The bijection is an isomorphism of groups with respect to addition on the torus and the usual collinear addition law on elliptic curves. Moreover, two complex tori are isomorphic if and only if the corresponding elliptic curves are isomorphic, and given any elliptic curve $y^2 = 4x^3 - a_2x - a_3$ with non-vanishing *cubic discriminant*, i.e. $a_2^3 - 27a_3^2 \neq 0$, there exists a lattice $L = \mathbb{Z}\tau + \mathbb{Z}$ such that $a_2 = g_2$ and $a_2 = g_3$. (The modular discriminant Δ is precisely $g_2^3 - 27g_3^2$.) It follows that isomorphism classes of complex tori correspond as algebraic objects to isomorphism classes of elliptic curves, and the conduit is precisely $\wp$.

We have provided more than sufficient background material to preface and motivate the next two sections, where we will present the main results of Chapters 2 and 3, respectively. In the next section we will look specifically at the Jacobi theta constant θ_3 and at its Taylor coefficients, while in Section 1.3 we will take a closer look at (1.4) and alternative regularizations.

1.2. Introduction to Chapter 2: Taylor coefficients of θ_3 and a conjecture of Romik

1.2.1. The sequence $(d(n))_{n=0}^{\infty}$ and our main contribution. In Chapter 2 we will establish congruence properties of the integer-valued sequence of normalized Taylor coefficients of θ_3, at the point $\tau = i/2$. The sequence was discovered by Romik [**Rom20**] and is defined below in Definition 1.2.2. The first several terms are given by

$$(d(n))_{n=0}^{\infty} = 1, 1, -1, 51, 849, -26199, 1341999, 82018251, 18703396449, \ldots$$

(see also [**SI20**]). Specifically, we will show:

Theorem 1.2.1.

(i) $d(n) \equiv 1 \pmod 2$ *for all* $n \geq 0$,

(ii) $d(n) \equiv (-1)^{n+1} \pmod 5$ *for all* $n \geq 1$,

(iii) if p *is prime and* $p \equiv 3 \pmod 4$, *then* $d(n) \equiv 0 \pmod p$ *for all* $n > \frac{p^2-1}{2}$.

This proves half of Conjecture 13 (b) in [**Rom20**], where the sequence $(d(n))$ was first introduced. The half of the statement that we do not prove is that for primes $p = 4k+1$, the sequence $(d(n))_{n=1}^{\infty}$ is periodic modulo p, although Theorem 1.2.1 is a specific example of this phenomenon in the case $p = 5$. (This gap was filled in [**GMR20**] shortly after the publication in [**Sch21**] of the results discussed here, thus proving the full conjecture of Romik – see Section 1.2.2.)

The sequence $(d(n))$ is defined in terms of the Jacobi theta constant θ_3, modified from Definition 1.1.2 in the following way.

Definition 1.2.1. Let θ be the holomorphic function defined on the right half-plane $\{x \in \mathbb{C} : \mathrm{Re}(x) > 0\}$ by

$$\theta(x) = 1 + 2\sum_{n=1}^{\infty} e^{-\pi n^2 x}. \tag{1.7}$$

Observe that $\theta(x) = \theta_3(ix/2)$, and that the modular transformation of θ_3 manifests for θ as

$$\theta\left(\frac{1}{x}\right) = \sqrt{x}\,\theta(x). \tag{1.8}$$

Definition 1.2.2 (Romik [**Rom20**]). Define the function σ on the unit disk by

$$\sigma(z) = \frac{1}{\sqrt{1+z}}\theta\left(\frac{1-z}{1+z}\right). \tag{1.9}$$

Then $(d(n))_{n=0}^{\infty}$ is given by

$$d(n) = \frac{\sigma^{(2n)}(0)}{A\Phi^n},$$

where $\Phi = \frac{\Gamma(\frac{1}{4})^8}{128\pi^4}$, and $A = \theta(1) = \frac{\Gamma(\frac{1}{4})}{\sqrt{2}\pi^{3/4}}$.

Thus, the numbers $(d(n))_{n=0}^{\infty}$ are the Taylor coefficients, modulo trivial factors, of σ at 0. It's not at all clear from the definition that the numbers $d(n)$ are integers, but this is shown to be true in [**Rom20**]. Furthermore, the connection of the sequence $(d(n))$ to the derivatives of θ at 1 can be made explicit:

Theorem 1.2.2 (Romik [**Rom20**]). *For all $n \geq 0$,*

$$\theta^{(n)}(1) = A \cdot \frac{(-1)^n}{4^n} \sum_{k=0}^{\lfloor n/2 \rfloor} \frac{(2n)!(4\Phi)^k}{2^{n-2k}(4k)!(n-2k)!} d(k). \tag{1.10}$$

1.2.2. Taylor coefficients of modular forms and connection to other work. The results presented here, which describe congruence properties of a specific integer sequence, may be viewed in the broader context of the study of arithmetic properties of Taylor coefficients of half-integer weight modular forms around complex multiplication points. Given a modular form f of weight k and a CM point $z \in \mathbb{H}$, rather than use the usual complex derivative $\frac{df}{dz}$, it is convenient to define the Taylor expansion of f in the following way (see e.g. Ch. 5.1 in [**Zag08**]). Set $f'(z) = (1/2\pi i)\frac{df}{dz}$ and define the differential operator ∂ by

$$\partial f(z) = (1/2\pi i) f'(z) - \frac{k}{4\pi \mathrm{Im}(z)} f(z).$$

The derivative ∂ has the advantage over f' of transforming like a modular form (of weight $k+2$), but at the cost of being holomorphic. Higher order derivatives ∂^n are defined recursively, i.e. $\partial^n = \partial \circ \partial^{n-1}$, with the convention that one treats the factor $1/\mathrm{Im}(z)$ as a constant when differentiating. The Taylor expansion of f at z is then expressed in terms of a new variable w in the unit disk, as

$$(1-w)^{-k} f(M(w)) = \sum_{n=0}^{\infty} c(n) \frac{w^n}{n!} \quad (|w| < 1), \tag{1.11}$$

where $c(n) = \partial^n f(z) \cdot (4\pi \mathrm{Im}(z))^n$, and M is the Möbius transformation given by $M(w) = \frac{z-\bar{z}w}{1-w}$, which maps the unit disk to $\mathbb{H}$ with $M(0) = z$. In the case of $\theta_3(z) = \theta(-2iz)$, the Taylor coefficients $c(n)$ in the above expansion about the CM point $z = i/2$ are the sequence $(d(n))$ (after a proper normalization) introduced in [**Rom20**] and studied here.

The congruences for $(d(n))$ that we consider are analogous to known congruences in the integer weight case. For example it was shown in [**LS14**] that if a prime p is inert in the CM-field generated by z, then the Taylor coefficients at z of a modular form with integer Fourier coefficients will eventually vanish modulo any positive power of p. In addition, the periodicity result in Theorem 1.2.1 for $p = 5$ has analogues for integer weight modular forms, which are known in general cases to have periodic coefficients modulo powers of p when p is a split prime (see e.g. [**DG08**]). However, similar results for weight 1/2 had not been established before the publication of the content in Chapter 2. Shortly afterward, the following theorem appeared in [**GMR20**].

THEOREM 1.2.3 (Guerzhoy, Mertens, Rolen (2019)). *Suppose $k, N \in \mathbb{N}$ and $f \in M_{k-\frac{1}{2}}(\Gamma_1(4N))$ is a modular form with algebraic Fourier coefficients, and p is a split prime in $\mathbb{Q}(\tau_0)$ for a CM point τ_0. Assume furthermore that the absolute norm of the algebraic number $G_2/(\zeta(2k)\theta_3(\tau_0))$ is p-integral and is not divisible by p. Then there exists $\Omega \in \mathbb{C}^\times$, which can be chosen to depend only on τ_0 and p, such that for $n_1, n_2 > A$ satisfying*

$$n_1 \equiv n_2 \,(\mathrm{mod}\,(p-1)p^A),$$

we have

$$\partial^{n_1} f(\tau_0)/\Omega^{2k+4n_1-1} \equiv \partial^{n_1} f(\tau_0)/\Omega^{2k+4n_2-1}\,.$$

The modular form space $M_{k-1/2}(\Gamma_1(4N))$ contains θ_3 in the case $k = 1$. The transcendental factor Ω is an algebraic multiple of the "Chowla-Selberg period" [**Zag08**, p. 84], which agrees with the normalization factor $A\Phi$ used in [**Rom20**] in the definition of $d(n)$. Theorems 1.2.1 and 1.2.3 together imply that Conjecture (b) of [**Rom20**] is true.

It is known in general [**Zag08**, Cor. 27] that Taylor coefficients (at a CM point) of a modular form f (with algebraic Fourier coefficients) are algebraic multiples of powers of the Chowla-Selberg period. What makes Romik's result more surprising then is that $(d(n))_{n=0}^{\infty}$ is a sequence of rational integers. While even the algebraic *integrality* of the Taylor coefficients that we have defined above is indicated (although without proof) in [**Zag08**] to hold generally, the degree being 1 in the case of $(d(n))$ is special.

Since, as the reader will see below in Theorem 2.1.1, the integers $(d(n))$ can be defined recursively in terms of the Taylor coefficients of a certain hypergeometric function, we point out that recurrence relations are known in general to produce the Taylor coefficients $\partial^n f(\tau)$ of modular forms near CM points τ. This is demonstrated in [**VD93**] for integer-weight forms and in [**GMR20**] for the half-integer weight case by a similar method, which does not bear an obvious resemblance to the derivation in [**Rom20**] of a recursion for $(d(n))$. In particular they relate the differential operators ∂^n to another differential operator, the *Serre derivitive*, which is defined for weight-k modular forms f by

$$\vartheta_k f(\tau) := (1/2\pi i)f'(\tau) - \frac{k}{\pi^2} G_2(\tau)f(\tau)\,,$$

and whose higher order iterates operate on the basis $\{E_4, E_6\}$ for $M_*(\Gamma)$ in a manner that can be described by a simple recurrence relation. The quasimodular behavior of the Eisenstein series G_2 is essential for the utility of ϑ_k in this regard.

One last remark is that congruence properties of the *Fourier coefficients* of modular forms, which can be regarded by the Fourier expansion as their derivatives at ∞, have been well-studied since the work of Ramanujan. He famously proved, for example, that $\tau(n) \equiv \sigma_{11}(n) \pmod{691}$, where $\sigma_{11}(n)$ is the sum of the 11^{th} powers of the positive divisors of n, and $\tau(n)$ denotes the n^{th} Fourier coefficient of the modular discriminant Δ introduced in Section 1.1.

1.3. Introduction to Chapter 3: Regularizations of the Eisenstein series G_2 and the Weierstrass $\wp$-function

In Chapter 3 we will show that the concept of "residual term" from (1.4) can be generalized to a much larger class of regularizations for the series defining G_2 and the Weierstrass $\wp$-function. In particular, we will assign to certain compact shapes in $\mathbb{R}^2$ the residual term that arises from partially summing the relevant infinite series over the integer lattice points (m, n) inside a scaled-up copy of the shape and taking the limit of these sums as the scaling factor goes to infinity, and we give an explicit formula for this residual term. In this introductory section we set up the relevant definitions and state the main result.

1.3.1. Shape summation. Denote by $\mathcal{K}$ the class of compact sets $K \subset \mathbb{R}^2$ that are convex, have nonempty interior and are symmetric about the x and y axes. (For simplicity we restrict the discussion to this class of shapes, although it is possible to consider things at a greater level of generality; see the final comment in Section 3.3.)

Definition 1.3.1. For each $K \in \mathcal{K}$ we define h_K to be the real-valued function whose graph is the upper boundary of the shape K. The function h_K is necessarily compactly supported on an interval of the form $[-A, A]$, is an even function, and its reflection $-h_K$ is the lower boundary of K.

Definition 1.3.2. For a shape $K \in \mathcal{K}$ and an array $(a_{m,n})_{m,n\in\mathbb{Z}}$ of complex numbers, we define

$$\sum_K a_{m,n} := \lim_{\lambda\to\infty} \sum_{(m,n)\in(\lambda K)\cap\mathbb{Z}^2} a_{m,n}, \tag{1.12}$$

provided the limit exists. We refer to this sum as the K-*summation*, or *shape summation with respect to the shape* K, of the array $(a_{m,n})$.

In the next definition we apply the concept of shape summation in a way that generalizes (1.3) in the definition of the Eisenstein series G_2.

Definition 1.3.3. If $K \in \mathcal{K}$, we denote by $G_2(K, \tau)$ the K-*summation of the weight-2 Eisenstein series*, defined as

$$G_2(K,\tau) := \sum_K \frac{1}{(m\tau + n)^2}, \tag{1.13}$$

provided the limit defining the summation exists, and with the convention that $a_{0,0} = 0$ in (1.12), to make allowance for the fact that the summand $\frac{1}{(m\tau+n)^2}$ is not defined for $m = n = 0$.

DEFINITION 1.3.4. If $K \in \mathcal{K}$ and $G_2(K,\tau)$ is defined, we denote by $E(K,\tau)$ the *residual function associated to* K, which is defined as

$$E(K,\tau) := G_2(K,\tau) - G_2(\tau).$$

With these definitions in place we have the following result, which gives an explicit formula for the residual function.

THEOREM 1.3.1. *For all $\tau \in \mathbb{H}$ and all $K \in \mathcal{K}$, the limit defining $G_2(K,\tau)$ exists. The residual function $E(K,\tau)$ is given by*

$$E(K,\tau) = 4\int_0^A \frac{h_K(x)}{\tau^2 x^2 - h_K^2(x)}\,dx \tag{1.14}$$

(where as before, A denotes a number for which h_K is supported on $[-A,A]$).

1.3.2. First example: the rectangle. Let us motivate the theorem by first considering the simplest example, namely when K is the rectangle $[-c,c] \times [-1,1]$ with aspect ratio c, for some $c > 0$. In this case, h_K is the indicator function $h_K(x) = \chi_{[-c,c]}(x)$. Evaluating the integral in (1.14) gives that

$$E(K,\tau) = G_2(K,\tau) - G_2(\tau) = -\frac{4}{\tau}\tanh^{-1}(c\tau).$$

In terms of the principal branch of the logarithm, the latter expression is

$$-\frac{2}{\tau}[\log(1+c\tau) - \log(1-c\tau)].$$

Note that we can interpret the limiting case $c \to 0$ of the shape summation (1.13) to represent a summation with respect to an "infinitely tall and narrow" rectangle, that is, first summing over n and then over m as in the original definition (1.3) of $G_2(\tau)$. The residual function in that case should be 0, and indeed we have that $\lim_{c\to 0} -\frac{4}{\tau}\tanh^{-1}(c\tau) = 0$. At the other extreme, we can interpret the case $c \to \infty$ to represent summing with respect to an "infinitely long and thin" rectangle, that is, first summing over m and then n. In this case we have that $\lim_{c\to\infty} -\frac{4}{\tau}\tanh^{-1}(c\tau) = -\frac{2\pi i}{\tau}$, and indeed this is consistent with the relation (1.4), which can now be understood as giving the residual function of such long and thin rectangles. Thus we see that summing with respect to rectangles provides a conceptual generalization of (1.4).

1.3.3. Shape summation of $\wp$. We can also consider shape summation for the series associated with the Weierstrass $\wp$-function (from Definition 1.2.2). We saw that the natural construction to try in searching for an elliptic function was $z \mapsto \sum_{m,n} \frac{1}{(z+n+m\tau)^2}$, but this suffers from dependence on the order of summation. This phenomenon can be generalized as follows.

Definition 1.3.5. For $K \in \mathcal{K}$ and $\tau \in \mathbb{H}$, we denote by $\wp(K, z)$ the K-summation

$$\wp(K, z) := \sum_{K} \frac{1}{(z+n+m\tau)^2} \qquad (z \notin \mathbb{Z}\tau + \mathbb{Z}),$$

provided the limit defining the summation exists. We refer to $\wp(K, z)$ as the *K-summation of the Weierstrass $\wp$-function.*

The next result shows that the limit defining $\wp(K, z)$ does exists, and that $\wp(K, z)$ is closely related to the residual function $E(K, \tau)$ and the weight-2 Eisenstein series G_2.

Theorem 1.3.2. *For $K \in \mathcal{K}$, $\tau \in \mathbb{H}$ and $z \notin \mathbb{Z}\tau + \mathbb{Z}$, $\wp(K, \tau)$ is defined and satisfies*

$$\wp(K, z) = \wp(z) + G_2(\tau) + E(K, \tau).$$

1.4. Introduction to Chapter 4: Asymptotic sharpness in tree enumeration and a conjecture of Kuperberg

1.4.1. Motivation from representation theory. We will analyze the sharpness of a certain estimate that occurs naturally in the asymptotic enumeration of rooted trees (see Definition 1.4.1 below). Our motivation is a particular problem from the literature, a conjecture formulated by Kuperberg in his study of the representation theory of simple rank-2 Lie algebras [**Kup96**, Conjecture 8.2].

Specifically, set $a_0 = 1$, and for each positive integer n, let a_n denote the number of triangulations of a regular n-gon, such that the minimum degree of each internal vertex is 6. The sequence begins

$$(a_n)_{n=0}^{\infty} = 1, 0, 1, 1, 2, 5, 15, 50, 181, 697, \ldots$$

and is indexed in the On-Line Encyclopedia of Integer Sequences (OEIS, [**SI20**]) by A059710.

Next, let $b_0 = 1$, and for each positive integer n, let $b_n = \dim_{G_2} \mathrm{Inv}(V(\lambda_1)^{\otimes n})$ be the dimension of the vector subspace of invariants in the n-th tensor power of the 7-dimensional fundamental representation of the exceptional simple Lie algebra G_2. We explain this briefly. Following [**Hum72**], we recall that the Lie algebra G_2 can be defined in various ways, among which are an abstract definition as the unique semi-simple Lie algebra (up to isomorphism) corresponding to the G_2 root system, and a concrete definition as a particular 14-dimensional Lie subalgebra of the 7×7 matrices over $\mathbb{C}$. G_2 has a 2-dimensional Lie subalgebra, the Cartan subalgebra, that acts via the adjoint representation as simultaneously diagonalizable endomorphisms of G_2. In general, the isomorphism classes of finite-dimensional irreducible representations of a semi-simple Lie algebra over $\mathbb{C}$ with Cartan subalgebra H are in bijection with the set Λ^+ of "dominant weights," which is a subset of the dual of H. In the case of G_2, λ_1 is a particular dominant weight whose corresponding representation $V(\lambda_1)$ is 7-dimensional. Taking an arbitrary tensor power of $V(\lambda_1)$, one can ask what is the dimension in $V(\lambda_1)^{\otimes n}$ of the subspace which is annihilated by G_2, where an element $x \in G_2$ acts on tensor products $v_1 \otimes v_2$ by $x(v_1 \otimes v_2) = xv_1 \otimes v_2 + v_1 \otimes xv_2$ and inductively by associativity on longer tensor products. The dimension of this subspace is b_n.

The sequence begins

$$(b_n)_{n=0}^{\infty} = 1, 0, 1, 1, 4, 10, 35, 120, 455, 1792, \ldots$$

and is indexed in OEIS as A059710.

The sequence (b_n) is also known to have a combinatorial interpretation as the number of lattice walks in the dominant Weyl chamber of the root system for G_2 – a $30°$ sector in the triangular lattice in $\mathbb{R}^2$ which serves as a geometric repsresentation for the set Λ^+ above – that start and end at the origin, subject to certain constraints on the steps [**Wes07**]. This type of model is not unique to G_2 or this particular representation. In general, if V is any irreducible representation of any complex semi-simple Lie algebra L, there is a similar lattice walk model for the dimension of the space of L-invariant n-tensors over V [**GM93**, Thm. 5].

Now let $A(x) = 1+\sum_{n=1}^{\infty} a_n x^n$ and $B(x) = 1+\sum_{n=1}^{\infty} b_n x^n$ be the ordinary generating functions for $(a_n)_{n=0}^{\infty}$ and $(b_n)_{n=0}^{\infty}$, respectively. In [**Kup96**, Section 8], Kuperberg proved the following remarkable identity of formal power series:

$$B(x) = A(xB(x)). \tag{1.15}$$

He also observed that $B(x)$ has radius of convergence $1/7$, that $B(1/7) < \infty$, and that by (1.15) $A(x)$ has radius of convergence at least $(1/7)B(1/7)$ (see Lemma 4.1.1 below), a constant whose numerical value he estimated to be approximately 6.811. He conjectured that this bound is in fact an equality.

Conjecture 1.4.1 (Kuperberg, 1996 [**Kup96**]).

$$\limsup_{n\to\infty} \sqrt[n]{a_n} = 7/B(1/7)\,.$$

1.4.2. Our main contributions. We prove Conjecture 1.4.1. Moreover, we explicitly identify the value of Kuperberg's constant $7/B(1/7)$ and go beyond the exponential growth term to establish a true asymptotic formula for (a_n) and a full asymptotic expansion for (b_n). The precise result is as follows.

THEOREM 1.4.1. *Let $A(x)$ and $B(x)$ be as above. Define constants ρ, K, and M by:*

$$\rho = \frac{7}{B(1/7)} \tag{1.16}$$

$$K = \frac{4117715\sqrt{3}}{864\pi} \approx 2627.6 \tag{1.17}$$

$$M = \frac{4\sqrt{3}}{421875\pi}\left(\frac{8575\pi - 15552\sqrt{3}}{2592\sqrt{3} - 1429\pi}\right)^7 \approx 1721.0 \tag{1.18}$$

Then we have the following:

(a) ***Kuperberg's conjecture is true.*** *As $n \to \infty$,*

$$a_n = \rho^{n+o(n)}. \tag{1.19}$$

(b) ***Explicit value of ρ.*** *The constant ρ has the explicit value*

$$\rho = \frac{5\pi}{8575\pi - 15552\sqrt{3}} \approx 6.8211. \tag{1.20}$$

(c) ***Asymptotic expansion of b_n.*** *As $n \to \infty$, the sequence (b_n) grows asymptotically as*

$$b_n = K\frac{7^n}{n^7}\left(1 + \mathcal{O}\left(\frac{1}{n}\right)\right). \tag{1.21}$$

Furthermore, there exists a computable sequence of rational numbers $(\kappa_i)_{i=7}^{\infty}$, with $\kappa_7 = K\pi/\sqrt{3}$, such that as $n \to \infty$,

$$b_n \sim \frac{7^n\sqrt{3}}{\pi}\sum_{i=7}^{\infty}\frac{\kappa_i}{n^i}. \tag{1.22}$$

(d) ***Asymptotic formula for a_n.*** *Conjecture 1.4.1 admits the following refinement. As $n \to \infty$,*

$$a_n = M\frac{\rho^n}{n^7}\left(1 + \mathcal{O}\left(\frac{\log n}{n}\right)\right). \tag{1.23}$$

We will also show in Corollary 4.3.1 that neither A nor B are algebraic.

1.4.3. A criterion for sharpness in tree enumeration and related analysis. Our proof of Theorem 1.4.1 will rely on several ideas that are far more general in their applicability than the case of the specific generating functions $A(x)$ and $B(x)$, and are of independent interest. Specifically, Conjecture 1.4.1 can be viewed as an asymptotic enumeration problem in the combinatorial theory of rooted trees, as (1.15) is a classic identity that encodes the recursive nature of these structures. We will have more to say about this in Section 1.4.4.

In general, if $A(x) = 1 + \sum_{n\geq 1} a_n x^n$ and $B(x) = 1 + \sum_{n\geq 1} b_n x^n$ are ordinary generating functions, with radii of convergence $R > 0$ and $r > 0$ respectively, and they satisfy (1.15), then the inequality $rB(r) \leq R$ holds if $a_n \geq 0$ for all $n \geq 1$ (see Lemma 4.1.1). It is natural then to ask when equality holds. We address this question in Section 4.1 and eventually arrive at a criterion for equality in the estimate $rB(r) \leq R$. A simplified version of this criterion reads as follows.

THEOREM 1.4.2 (Criterion for sharpness, simplified version). *With $A(x)$, $B(x)$, R, and r as in the preceding paragraph, assume that $a_n \geq 0$ for all $n \geq 1$ and that gcd$\{n \geq 1 : a_n > 0\} = 1$. Then*

$$b_n r^n \neq \Theta(n^{-3/2}) \text{ as } n \to \infty \implies R = rB(r)\,.$$

Kuperberg's conjecture will follow from this criterion, since a formula from the character theory of Lie algebra representations will lead us to the preliminary estimate $b_n/7^n = \Theta(n^{-7})$ for the sequence (b_n) in Conjecture 1.4.1 (see Section 4.2). For the full criterion, including some technical details, see Theorem 4.1.3 in Section 4.1.

Another batch of concepts of general interest is the singularity analysis conducted in Section 4.3, by which we study a new formula from [**BTWZ19**] for the generating function $B(x)$ in Conjecture 1.4.1 and prove the remaining parts of Theorem 1.4.1. In particular, we apply the "transfer theorem" approach of Flajolet and Odlyzko (see Section 1.4.5). The fact that $rB(r) = R$ for this example (Conjecture 1.4.1) leads to rather subtle analysis in the application of this approach when compared to the more well-studied case of $rB(r) < R$. Example 4.1.2 and the remark that follows it may further clarify this perspective.

1.4.4. Simply generated trees. Let $A(x) = 1 + \sum_{n\geq 1} a_n x^n$ and $B(x) = 1 + \sum_{n\geq 1} b_n x^n$ be power series satisfying (1.15). When $B(x)$ has a positive radius of convergence, we would like to know when the identity (1.15) of formal power series is also an identity of the complex functions defined by these power series in a neighborhood of the origin, since then we may apply analytic methods. A sufficient condition is non-negativity of the coefficients – see Lemma 4.1.1. We will adopt a useful convention of setting $y(x) := xB(x)$, whereby the identity (1.15) can be rewritten as

$$y(x) = xA(y(x)). \tag{1.24}$$

The coefficient sequence $(y_n)_{n=1}^{\infty}$ of $y(x) = \sum_{i\geq 1} y_i x^i$ is then given simply as $y_n = b_{n-1}$, for $n \geq 1$.

The functional equation (1.24) has a well-known interpretation in the theory of rooted trees.

DEFINITION 1.4.1. A *planar rooted tree* is an undirected acyclic graph, equipped with a distinguished node and an embedding in the plane (so that distinct subtrees dangling from the same node are ordered amongst themselves). A family of planar rooted trees is called *simply generated* (see [**MM78**], where this nomenclature appears to have been introduced) if the number of trees in the family is counted by a generating function $y(x)$ that satisfies (1.24) for some $A(x) = 1 + \sum_{n\geq 1} a_n x^n$ with non-negative coefficients.

The following combinatorial interpretation is classical.

THEOREM 1.4.3. *Suppose that $A(x) = 1 + \sum_{n\geq 1} a_n x^n$, where $(a_n)_{n\geq 1}$ is a sequence of non-negative integers, and $y(x) = \sum_{n\geq 1} y_n x^n$ is related to $A(x)$ via (1.24). Then y_n is the number of planar rooted trees with n nodes (including the root), such that for each $i \geq 1$, an internal node having i children can be colored with one of a_i distinct colors.*

PROOF SKETCH. We can think of a tree of n nodes as being built recursively by attaching k subtrees to a root node for some $k > 0$, such that the total number of nodes among the k subtrees is $n-1$. One then sees that the coefficients (y_n) in the generating function identity satisfy the same recurrence relation as the number of trees of the described type, which is that $y_1 = 1$ and that for $n \geq 1$,

$$y_n = \sum_{k=1}^{n-1} a_k p(n,k)\,,$$

where

$$p(n,k) := \sum_{\lambda} \left(\prod_{i=1}^{k} y_{\lambda_i} \right)\,,$$

with the sum running over all unordered partitions $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_k)$ of $n-1$ into k positive parts, i.e. $\lambda_1 + \lambda_2 + \cdots + \lambda_k = n-1$. (Partitions are reviewed briefly at the beginning of Section 2.2.) $\square$

The article [**Drm04**] contains several examples of (1.24) and a concise explanation of some fundamental asymptotic results, including that the Catalan numbers occur as the sequence $(y_n)_{n=1}^{\infty}$ when $A(x) = 1/(1-x)$, and in that case $y_n \sim \pi^{-\frac{1}{2}} 4^{n-1} n^{-\frac{3}{2}}$ as $n \to \infty$ (see Example 4.1.1 below). Generalization of the functional equation (1.24) are also discussed, as well as statistical analysis of parameters associated to trees, such as their expected number of leaves. The text [**FS09**, Sec. VI.7, VII.3, VII.4] contains a broad treatment of the analytic framework for the functional equation (1.24), which expands our discussion in 4.1, and includes asymptotic results by way of singularity analysis applied to many natural tree examples from the literature. We give one example in the next section.

1.4.5. Transfer theoerems. We recall here as Theorem 1.4.4 the famous "transfer theorems" of Flajolet and Odlyzko [**FO90**], which we will use to transfer asymptotic growth estimates of a function f near a dominant singularity to asymptotic growth estimates for the function's Taylor coefficients $(f_n)_{n\geq 0}$.

Definition 1.4.2 ([**FO90**]). Let f be a function analytic at the origin, with radius of convergence $R > 0$. We say that f *can be continued analytically to a Delta-domain* if f extends analytically to an open set Δ_R of the form

$$\{z : |z| < R + \epsilon, |\mathrm{Arg}(z - R)| > \theta\},$$

for some $\epsilon > 0$ and some $\theta \in (0, \pi/2)$, where Arg denotes the principle value of the argument. In particular, implied by the definition is that f has a unique singularity on its disk of convergence, namely the point R. We may also refer to Δ_R as a *Delta-domain around the disk of convergence of f*.

In practical applications of the following result, functions often extend analytically well-beyond a Delta-domain, e.g. to $\mathbb{C} \setminus [R, \infty)$.

Theorem 1.4.4. *[**FO90**, Cor. 2 and Thm 2] Assume that f can be continued analytically to a Delta-domain Δ_R. Denote the principle branch of the logarithm by* log.

(1) If $f(z) \sim K(1 - z/R)^{\alpha}$ as $z \to 1$ in Δ_R, where $\alpha \in \mathbb{C} \setminus \{0, 1, 2, \dots\}$, and $K \in \mathbb{C}$, then

$$f_n \sim \frac{1}{R^n} \cdot \frac{K}{\Gamma(-\alpha)} n^{-\alpha-1}, \qquad \text{as } n \to \infty.$$

(2) If $f(z) = \mathcal{O}((1 - z/R)^\alpha(\log(1 - z/R))^\gamma)$ as $z \to R$ in Δ_R, where $\alpha, \gamma \in \mathbb{R}$, then

$$f_n = \mathcal{O}\left(\frac{1}{R^n}(n^{-\alpha-1})(\log n)^\gamma\right), \qquad \text{as } n \to \infty.$$

(3) As a consequence of (1) and (2), if $F(z) = g(z) + f(z)$, for f and g analytic on $\{z : |z| < R\}$, and furthermore $f(z)$ is analytic in a Delta-domain Δ_R and satisfies

$$f(z) = \mathcal{O}\big((1 - z/R)^\alpha(\log(1 - z/R))^\gamma\big),$$

as $z \to R$ in Δ_R, then

$$F_n = g_n + f_n = g_n + \mathcal{O}\left(\frac{n^{-\alpha-1}(\log n)^\gamma}{R^n}\right).$$

Theorem 1.4.4 will be used in Section 4.3 to get asymptotic estimates for the sequences (a_n) and (b_n) of Theorem 1.4.1, with $\gamma = 1$ in both cases. The theorem is actually stated and proved in [**FO90**] for the special case $R = 1$, and the adjustments above for general $R > 0$ are simple.

These transfer theorems and their variants have proven to be an indispensable toolkit for doing analytic combinatorics. A whole chapter in [**FS09**] is devoted to developing a systematic procedure for tackling asymptotic problems by these methods (see also [**Drm04**]). We give one example now, which ties together Theorems 1.4.3 and 1.4.4.

Example 1.4.1. Let $(y_n)_{n=0}^\infty$ count the number of planar rooted trees with $n + 1$ nodes, such that each node has 0, 1, or 2 children. Then with $A(x) = 1 + x + x^2$, we have the following generating function identity.

$$y(x) = xA(y(x)) = 1 + xy(x) + xy(x)^2$$

(In terms of Theorem 1.4.3, there is 1 color allowed for nodes with less than 3 children, and 0 colors allowed otherwise). Solving for y we obtain

$$y(z) = \frac{1 - z - \sqrt{(1 - 3z)(1 + z)}}{2z} = \frac{1 - z}{2z} - \sqrt{1 - 3z} \cdot \frac{\sqrt{z + 1}}{2z},$$

where the principal branch of the square root is used. The singularity of smallest modulus is $z = 1/3$. It follows that y_n grows like 3^n. But what about sub-exponential growth? The expression involving square roots shows that y is analytic on $\mathbb{C} \setminus ((\infty, -1] \cup [1/3, \infty))$, so in particular on a

Delta-domain around the disk of convergence $\{z : |z| < 1/3\}$. Furthermore, as $z \to 1/3$ we have

$$\begin{aligned}
y(z) &= \frac{1 - z - \sqrt{(1-3z)(1+z)}}{2z} = \frac{1-z}{2z} - \sqrt{1-3z} \cdot \frac{\sqrt{z+1}}{2z} \\
&= \left[1 + \frac{3}{2}(1-3z) + \mathcal{O}(1-3z)^2\right] \\
&\quad - (1-3z)^{1/2}\left[\sqrt{3} + \frac{7\sqrt{3}}{8}(1-3z) + \mathcal{O}(1-3z)^2\right] \\
&= 1 - \sqrt{3}(1-3z)^{1/2} + \frac{12+7\sqrt{3}}{8}(1-3z) + \mathcal{O}(1-3z)^{3/2}.
\end{aligned}$$

Since $y(z) - 1 - (1-3z) = -\sqrt{3}(1-3z)^{1/2} + \mathcal{O}(1-3z)^{3/2}$, we see by the transfer theorem that as $n \to \infty$,

$$y_n = \frac{-\sqrt{3} \cdot 3^n}{\Gamma(-1/2)n^{3/2}} + \mathcal{O}\left(\frac{3^n}{n^2}\right) = \frac{3^{n+1/2}}{2\sqrt{\pi} \cdot n^{3/2}}\left(1 + \mathcal{O}\left(\frac{1}{n}\right)\right).$$

Moreover, by taking higher order terms in the Taylor expansions above and applying Theorem 1.4.4 to each fractional power of $(1-3z)$, one can obtain an asymptotic formula for y_n of arbitrarily high precision.

Theorem 1.4.4 is used in Examples 4.1.1 and 4.1.2 of Chapter 4 and in proving Theorem 1.4.1 parts (c) and (d). In the case of part (d), the verification of analytic extension to a Delta-domain is much more involved than in the other examples. We hope that the techniques that we use there will be helpful to other researchers in future applications.

1.5. Introduction to Chapter 5: Expectation of the sum of binary digits in the iterated Syracuse map

We shall make a small contribution to one of the most infamous problems in number theory, which is to predict the trajectory of positive integers through orbits of the Collatz map.

DEFINITION 1.5.1. The *Collatz map* $\mathcal{C} : \mathbb{N} \to \mathbb{N}$ is defined by

$$\mathcal{C}(N) = \begin{cases} 3N+1 & \text{if } n \text{ is odd} \\ N/2 & \text{if } n \text{ is even} \end{cases}$$

DEFINITION 1.5.2. For a function f defined on a subset $S \subset \mathbb{N}$ and for any $N \in S$, the *orbit* of N (under the action of f) is defined to be the sequence of iterates $(f^k(N))_{k=1}^{\infty}$, where $f^k := f \circ f \circ \cdots \circ f$ (k times).

The *Collatz conjecture* states that every orbit assumes the value 1 eventually (and hence infinitely often). In every orbit of the Collatz map, odd numbers are followed by even numbers, but not the other way around. The erratic distribution of strings of even numbers in any given orbit is essentially what makes the Collatz map difficult to understand. This is related to the mixing property of $\mathcal{C}$ when viewed as a map on the 2-adic integers $\mathbb{Z}_2$.

One general class of results deals with orbits of points N that are "localized in space." That is, if we restrict our attention to a bounded subset S of $\mathbb{N}$, what can we say about $\lim_{k\to\infty} \mathcal{C}^k(N)$? The state of the art is the following.

THEOREM 1.5.1 (Tao, 2020 [Tao20]). *Let $f : \mathbb{Z}^+ \to \mathbb{R}$ be any function with $\lim_{N\to\infty} f(N) = \infty$. Then for almost all $N \in \mathbb{Z}^+$ (in the sense of logarithmic density), $f(N)$ exceeds the minimum value in the orbit of N under $\mathcal{C}$, i.e.*

$$\inf_{k\geq 0} (\mathcal{C}^k(N)) < f(N)\,.$$

Before this theorem emerged the best known result was that $\pi_1(N) > N^{0.84}$, where $\pi_1(N)$ is defined for $N \in \mathbb{Z}^+$ as the number of positive integers less than N [KL03].

Another class of results is concerned with behavior "localized in time." For example, one considers what can be said about $\mathcal{C}(N)$ or $\mathcal{C}(N)^2$ for all $N \in \mathbb{N}$, either deterministically or probabilistically.

Our contributions are of this type. For a survey of known results, history, and methods regarding the Collatz conjecture and related problems, one may refer to [**Lag85**] and [**Lag10**].

In Chapter 5 we will study the following modification of $\mathcal{C}$, which is defined on the odd natural numbers $\mathbb{N}_{\mathrm{odd}}$ and neatly combines the two cases in the definition of the Collatz map. Let $\omega(N)$ be the *base-2 valuation* of a positive integer N, i.e. $\omega(N) = \sup_{k\geq 0}\{N/2^k \in \mathbb{Z}\}$.

Definition 1.5.3. The *Syracuse map* $\mathcal{S} : \mathbb{N}_{\mathrm{odd}} \to \mathbb{N}_{\mathrm{odd}}$ is defined by

$$\mathcal{S}(N) = \frac{3N+1}{2^{\omega(3N+1)}}\,.$$

We will give explicit formulas for the average sum of binary digits in the first two iterates of $\mathcal{S}$. To state the precise results we first introduce some notation.

Definition 1.5.4. Define the function $\sigma : \mathbb{N} \to \mathbb{N}$ by

$$\sigma(N) := \sum_{i=0}^{\infty} t_i,$$

where $N = \sum_{t=0}^{\infty} t_i 2^i$ is the binary expansion of N (i.e. $t_i \in \{0,1\}$ for all i). For $n \in \mathbb{Z}^+$, let N_n be a uniform random variable with values in $\mathbb{N}_{\mathrm{odd}} \cap [1, 2^n - 1]$. Let $(D_n)_{n=1}^{\infty}$ be the sequence defined by

$$D_n := \mathbb{E}[\sigma(N_n) - \sigma(S(N_n))],$$

and let $(E_n)_{n=1}^{\infty}$ be the sequence defined by

$$E_n := \mathbb{E}[\sigma(N_n) - \sigma(S^2(N_n))].$$

The numbers D_n and E_n can be interpreted as the average loss of "complexity" (in the information theoretic sense of nonzero bits) in the first iterate and second iterate respectively of the Syracuse map applied to a random odd integer in $[1, 2^n - 1]$. The initial values are as follows:

$$(D_n)_{n=1}^{\infty} = 0, 0, \frac{1}{4}, \frac{1}{4}, \frac{5}{16}, \frac{5}{16}, \frac{21}{64}, \frac{21}{64}, \ldots$$
$$(E_n)_{n=1}^{\infty} = 0, \frac{1}{2}, \frac{3}{4}, \frac{5}{8}, \frac{1}{2}, \frac{17}{32}, \frac{35}{64}, \frac{71}{128}, \ldots$$

Moreover, we have the following explicit formulas for (D_n) and (E_n).

THEOREM 1.5.2 (First iterate of $\mathcal{S}$). *For $n \geq 1$,*

$$D_n = \frac{1}{3} - \frac{3 + (-1)^n}{3 \times 2^n}\,. \tag{1.25}$$

By passing to the limit we can immediately make a simple heuristic interpretation: the image under $\mathcal{S}$ of a random positive odd integer N will on average possess $1/3$ fewer 1's that N possesses in its binary expansion.

THEOREM 1.5.3 (Second iterate of $\mathcal{S}$). *Define the periodic sequence*

$$(b_n)_{n=0}^{\infty} := \overline{(-7, -5, -1, 7, 5, -8)}\,.$$

For $n \geq 1$,

$$E_n = \frac{5}{9} + \frac{b_n}{9 \times 2^{n-1}}\,. \tag{1.26}$$

Theorems 1.5.2 and 1.5.3 appear to generalize to higher iterates of $\mathcal{S}$. For example, the following result was discovered experimentally by Romik [**RS**]:

CONJECTURE 1.5.1 (Third iterate of $\mathcal{S}$). *Define the periodic sequence*

$$(c_n)_{n=0}^{\infty} := \overline{(17, 8, 6, 10, 9, 8, -1, 2, -6, 1, -15, 23, 8, -22, -18, 10, -3, 20)}.$$

For $n \geq 1$,

$$\mathbb{E}[\sigma(N_n) - \sigma(S^3(N_n))] = \frac{7}{9} - \frac{k^2 - 3k - 2c_n}{9 \times 2^n}\,.$$

Note that we have overloaded notation in this dissertation – the sequences (b_n) and (c_n) have nothing to do with the sequences in Chapter 4.

Our approach to proving Theorems 1.5.2 and 1.5.3 in Chapter 5 is to represent the arithmetic operation $N \mapsto 3N + 1$ for a random odd natural number N as a finite-state machine, that is, as a random process on a finite graph whose steps are independent Bernoulli(1/2) random variables corresponding to the random binary digits in N. The authors of [**RS**] have developed a method to prove Conjecture 1.5.1 that improves on the strategy used here for the first two iterates of $\mathcal{S}$. They replace a key conditioning step and total expectation formula (see Section 5.3.4) with a conceptually simpler model involving linking together several finite-state machines. In theory this model can be used to study higher iterates of $\mathcal{S}$. The details are still in progress and will be formalized in the future. The conditional expectation approach used here, while not generalizing well to $\mathcal{S}^3$ or beyond, is perfectly adequate for handling the case of $\mathcal{S}^2$.

Our finite-state machine framework in Chapter 5 is not new. Similar models have been used to study limiting behavior for orbits of certain generalizations of $\mathcal{C}$ to p-partite functions defined for each N according to the congruence class of N modulo p. (See the survey [**Mat10**] above and the works cited there for more information.) These maps in turn extend to ergodic maps of the p-adic integers. We do not adopt the latter perspective here, although it may be fruitful in future work to extend our methods to $\mathbb{Z}_2$ to look for a general statement about the limiting behavior of infinite orbits of $\mathcal{S}$.

CHAPTER 2

Congruences for the Taylor coefficients of θ_3

Before beginning the proof of Theorem 1.2.1 we recall two further objects from [**Rom20**], an infinite array and a recurrence relation satisfied by $(d(n))_{n=0}^{\infty}$.

2.1. The auxiliary matrix $(s(n,k))_{1\le k\le n}$ and a recurrence relation for $(d(n))_{n=0}^{\infty}$

DEFINITION 2.1.1. Define the sequences $(u(n))_{n=0}^{\infty}$ and $(v(n))_{n=0}^{\infty}$ by $u(0) = v(0) = 1$ and the following recurrence relations for $n \ge 1$:

$$u(n) = (3\cdot 7\cdots(4n-1))^2 - \sum_{m=0}^{n-1}\binom{2n+1}{2m+1}(1\cdot 5\cdots(4(n-m)-3))^2\,u(m)\,, \tag{2.1}$$

$$v(n) = 2^{n-1}\,(1\cdot 5\cdots(4n-3))^2 - \frac{1}{2}\sum_{m=1}^{n-1}\binom{2n}{2m}v(m)v(n-m). \tag{2.2}$$

Additionally, define the infinite array $s = (s(n,k))_{1\le k\le n}$ as follows:

$$s(n,k) = \frac{(2n)!}{(2k)!}[z^{2n}]\left(\sum_{j=0}^{\infty}\frac{u(j)}{(2j+1)!}z^{2j+1}\right)^{2k}, \tag{2.3}$$

where $[z^n]f(z) = [z^n]\sum_{n=0}^{\infty} c_n z^n$ denotes the n^{th} coefficient c_n in a power series expansion for f. Finally, define $r(n,k) := 2^{n-k}s(n,k)$ for $1 \le k \le n$.

The numbers $r(n,k)$ were introduced in [**Rom20**] – and shown to be integers – along with the following recurrence relation for $d(n)$, which was used there to prove that $(d(n)) \subset \mathbb{Z}$.

THEOREM 2.1.1. *For all pairs (n,k), $1 \le k \le n$, both $r(n,k)$ and $s(n,k)$ are integers. Furthermore, with $d(0) = 1$, the following recurrence relation holds for all $n \ge 1$:*

$$d(n) = v(n) - \sum_{k=1}^{n-1} r(n,k)d(k). \tag{2.4}$$

The rest of this chapter is organized as follows. In **Section** 2.2 we derive new formulas for $s(n,k)$ and $s(n,k)$ modulo p. In **Section** 2.3 we give a simple proof of Theorem 1.2.1, part (i). In **Section** 2.4 and **Section** 2.5 we give proofs of parts (ii) and (iii), respectively, based on the expression for $s(n,k)$ mod p derived in Section 2.2, the recursion (2.4), and a few more facts about the congruences of $(u(n))$ and $(v(n))$.

2.2. Reduction of $s(n,k)$ modulo p

We briefly recall some standard definitions and facts regarding integer partitions. Let n and k be positive integers. By an *unordered partition* λ *(of* n *with* k *parts)* we mean, as usual, a tuple of positive integers, $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_k)$, with $\lambda_i \leq \lambda_{i+1}$ for $1 \leq i < k$, such that $\sum_{i=1}^{k} \lambda_i = n$. The numbers λ_i are the *parts*. We let $\mathcal{P}_{n,k}$ denote the set of unordered partitions of n with k parts, and we let $\mathcal{P}'_{n,k} \subset \mathcal{P}_{n,k}$ be the set of such partitions whose parts are odd numbers. For a given $\lambda \in \mathcal{P}_{n,k}$, we will let c_i denote the number of parts (possibly zero) of λ whose value is i, for $1 \leq i \leq n$. Thus, the tuple $c(\lambda) = (c_1, c_2, \ldots, c_n)$ gives an alternative description of λ, which we will use freely. (Although each c_i depends on λ, we choose not to reflect this dependence in the notation, in order to keep it simple and since it will always be clear from context.) Finally, observe that $\sum_{i=1}^{n} ic_i = n$, and $\sum_{i=1}^{n} c_i = k$, for each $\lambda \in \mathcal{P}_{n,k}$.

Lemma 2.2.1 ([**And76**, pp. 215-216]). *For a pair* (n,k) *of positive integers with* $n \geq k$*, and any partition* $\lambda \in \mathcal{P}_{n,k}$*, define the number* N_λ *by*

$$N_\lambda = \frac{n!}{\prod_{i=1}^{n} i!^{c_i} c_i!} .$$

Then N_λ *is an integer.*

In fact if S is a set with n elements, then N_λ is the number of set partitions of S into k blocks B_i, with $|B_i| \leq |B_{i+1}|$ for $1 \leq i < k$, such that $|B_i| = \lambda_i$. But we will not use this interpretation.

Now we derive a formula for reduction modulo p of $s(n,k)$.

Theorem 2.2.1. *For any pair* (n,k) *of positive integers such that* $n \geq k$*, we have*

$$s(n,k) = \sum_{\lambda \in \mathcal{P}'_{2n,2k}} \left[\frac{(2n)!}{\prod_{i=1}^{2n} i!^{c_i} c_i!} \prod_{i=1}^{2n} u\left(\frac{i-1}{2}\right)^{c_i} \right] = \sum_{\lambda \in \mathcal{P}'_{2n,2k}} \left[N_\lambda \prod_{i=1}^{2n} u\left(\frac{i-1}{2}\right)^{c_i} \right]. \tag{2.5}$$

Proof. We first observe that $\mathcal{P}'_{2n,2k} \neq \emptyset$, since if $n > k$ then $\mathcal{P}'_{2n,2k}$ contains the partition λ such that $c(\lambda)$ has $c_1 = 2k-1, c_{2n-2k+1} = 1$, and $c_i = 0$ for all other i; while if $n = k$, then $\mathcal{P}'_{2n,2k}$ contains λ with $c(\lambda) = (2k, 0, \ldots, 0)$. From (2.3) we see that

$$s(n,k) = \frac{(2n)!}{(2k)!}[z^{2n}] \left(\sum_{\substack{j \geq 1 \\ j \text{ odd}}} \frac{u\left(\frac{j-1}{2}\right)}{j!} z^j \right)^{2k}$$

$$= \frac{(2n)!}{(2k)!} \sum_{(j_1, j_2, \ldots, j_{2k})} \prod_{i=1}^{2k} \frac{u\left(\frac{j_i - 1}{2}\right)}{j_i!}, \tag{2.6}$$

where the sum runs over all tuples $j = (j_1, j_2 \ldots, j_{2k})$ of positive odd integers such that $\sum_{i=1}^{2k} j_i = 2n$ (in other words, over all *ordered partitions* of $2n$ into $2k$ odd parts). Call the set of such tuples $\Lambda_{2n,2k}$. Since $\mathcal{P}'_{2n,2k}$ is nonempty, so is $\Lambda_{2n,2k}$. To each $j \in \Lambda_{2n,2k}$ we associate the unique unordered partition $\lambda \in \mathcal{P}'_{2n,2k}$ obtained by ordering the j_i's in non-decreasing order, and we also associate the tuple $c(\lambda)$. We can define an equivalence relation on $\Lambda_{2n,2k}$ by calling j and j' equivalent if they map to the same $c(\lambda)$ under this association. If j maps to $c(\lambda) = (c_1, \ldots, c_{2n}) \in \mathcal{P}'_{2n,2k}$, then it is elementary to count that the size of the equivalence class of j is $\frac{(2k)!}{\prod_{i=1}^{2n} c_i!}$. Furthermore, the product $\prod_{i=1}^{2k} \frac{u\left(\frac{j_i-1}{2}\right)}{j_i!}$ in (2.6), as a function of $(j_1, \ldots, j_{2k})$, is constant on equivalence classes, and the equivalence classes are indexed by $\mathcal{P}'_{2n,2k}$ in the obvious way. Thus, we may rewrite (2.6) as

$$s(n,k) = \frac{(2n)!}{(2k)!} \sum_{\lambda \in \mathcal{P}'_{2n,2k}} \left(\frac{(2k)!}{\prod_{i=1}^{2n} c_i!} \prod_{i=1}^{2n} \frac{u\left(\frac{i-1}{2}\right)^{c_i}}{i!^{c_i}} \right),$$

which simplifies to (2.5). $\square$

For the rest of this chapter, if $x \in \mathbb{Z}$, and $p \geq 2$ is prime, we let x_p denote the congruence class of x modulo p. In light of Lemma 2.2.1 and the fact that each $u(n)$ is an integer, we see from (2.5) that $s(n,k) \in \mathbb{Z}$ for $1 \leq k \leq n$. More specifically, the summands in (2.5) are products of integers, so we may easily reduce them modulo p to obtain the following formula for $s(n,k)_p$.

Corollary 2.2.1. *For any pair (n,k) of positive integers such that $n \geq k$, and any prime number p, we have*

(2.7)
$$s(n,k)_p = \sum_{\lambda \in \mathcal{P}'_{2n,2k}} \left(\left[\frac{(2n)!}{\prod_{i=1}^{2n} i!^{c_i} c_i!} \right]_p \prod_{i=1}^{2n} \left[u\left(\frac{i-1}{2}\right)^{c_i} \right]_p \right) = \sum_{\lambda \in \mathcal{P}'_{2n,2k}} \left((N_\lambda)_p \prod_{i=1}^{2n} \left[u\left(\frac{i-1}{2}\right)^{c_i} \right]_p \right),$$

where the multiplication in parentheses is of congruence classes, as is the summation over $\mathcal{P}'_{2n,2k}$.

2.3. Proof of Theorem 1.2.1 (i): The case $p = 2$

In the previous section we saw that $s(n,k) = r(n,k)/2^{n-k}$ is an integer for all $1 \leq k \leq n$, which immediately implies that $r(n,k)$ is even. Thus, by (2.4), in order to show that $d(n)$ is odd for all n it suffices to show that $v(n)$ is odd for all n. We will prove this by induction. The first few values of $v(n)$ are given by $(v(n))_{n=0}^{\infty} = 1, 1, 47, 7395, \ldots$, which can easily be computed.

Assume now the induction hypothesis that $v(m)$ is odd for all $1 \leq m < n$. We will write $A \equiv B$, for $A, B \in \mathbb{Z}$, to mean that A and B have the same parity. We apply the induction hypothesis to simplify the expression in (2.2), obtaining

$$v(n) \equiv \frac{1}{2} \sum_{m=1}^{n-1} \binom{2n}{2m} = \frac{1}{2}\left[\left(\sum_{m=0}^{n} \binom{2n}{2m} \right) - 2 \right]. \tag{2.8}$$

Since

$$\begin{aligned} \sum_{m=0}^{n} \binom{2n}{2m} &= \frac{1}{2}\left[\left(\sum_{m=0}^{2n} \binom{2n}{m} \right) + \sum_{m=0}^{2n} \left(\binom{2n}{m} (-1)^m \right) \right] \\ &= \frac{1}{2}[2^{2n} + 0], \end{aligned}$$

we see from (2.8) that $v(n) \equiv 2^{2n-2} - 1 \equiv 1$, as was to be shown.

2.4. Proof of Theorem 1.2.1 (ii): Periodicity of $d(n)$ modulo $p = 5$

2.4.1. A formula for $r(n,k)$ mod 5. Corollary 2.2.1 provides a flexible way to reduce $s(n,k)$ – and hence $r(n,k)$ – modulo p, and will be our main tool along with the recurrence relation (2.4) to study the congruences of $d(n)$ modulo primes $p \neq 2$. In the case $p = 5$, the reduction (2.7) is particularly simple. Throughout this section the notation $A \equiv B$ will be shorthand for $A \equiv B \pmod 5$.

Theorem 2.4.1 (Formula for $r(n,k)$ mod 5). *For $1 \le k \le n \le 5k$ the following congruences hold mod 5:*

$$r(n,k) \equiv \begin{cases} \dfrac{(2n)!}{(\frac{5k-n}{2})!(\frac{n-k}{2})!5^{\frac{n-k}{2}}} & \text{if } n-k \text{ is even} \\[2ex] \dfrac{2(2n)!}{(\frac{5k-n-1}{2})!(\frac{n-k-1}{2})!5^{\frac{n-k-1}{2}}} & \text{if } n-k \text{ is odd} \end{cases} \tag{2.9}$$

If $n > 5k$, then $r(n,k) \equiv 0$.

A graphical plot of Theorem 2.4.1 shows a compelling fractal pattern (see Figure 2.1 below).

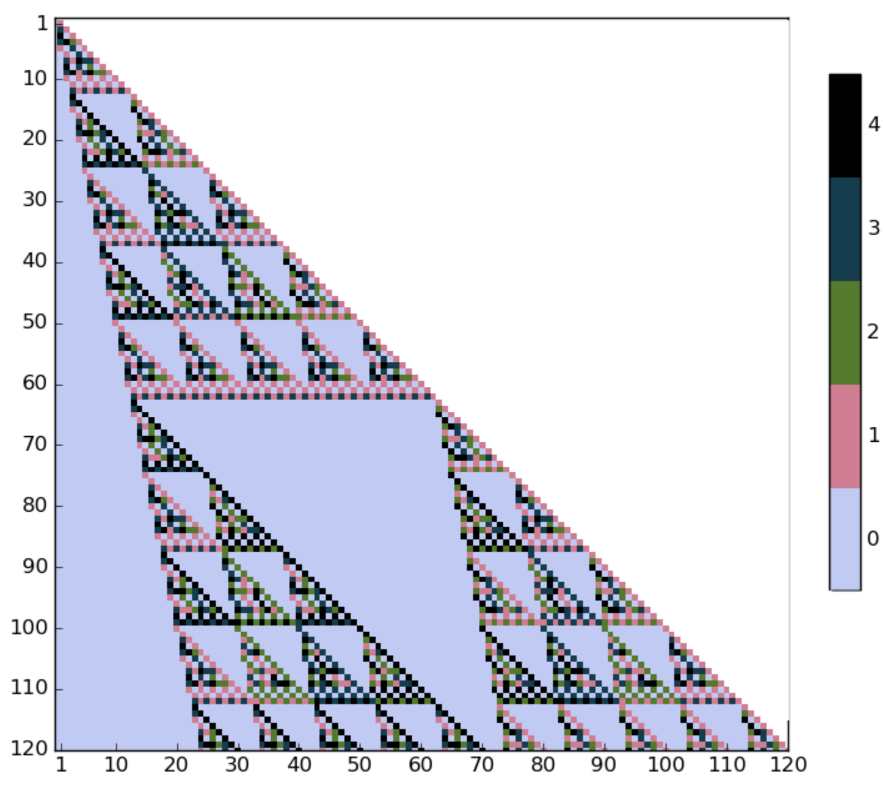


Figure 2.1. Congruences of $r(n,k)$ mod 5, $1 \le k \le n < 120$. The rows are indexed by n, the columns are indexed by k, and the colors indicate residue classes of $r(n,k)$ mod 5, according to the colorbar.

Before we begin the proof, we need another lemma about the sequences $(u(n))$ and $(v(n))$.

Lemma 2.4.1. *The sequences u and v satisfy the following congruences mod 5:*

$$(i) \qquad (v(n))_{n=0}^{\infty} \equiv (1,1,2,0,0,0,0,\dots)$$

$$(ii) \qquad (u(n))_{n=0}^{\infty} \equiv (1,1,1,0,0,0,0,\dots)$$

Proof. From Definition 2.1.1, one can easily calculate that the first few terms of the sequence $(u(n))_{n=0}^{\infty}$ are $1, 6, 256, 28560, 6071040$. Furthermore, it is clear from (2.1) that if $n \geq 4$ we have the simplified recursion

$$u(n) \equiv \binom{2n+1}{2n-1} u(n-1),$$

since the term $(3 \cdot 7 \cdot 11 \cdots (4n-1))^2)$ vanishes, as do all of the terms in the summation except for the term corresponding to $m = n-1$. Then by induction we see that $u(n) \equiv 0$ for all $n \geq 4$.

Similarly the initial terms of the sequence $(v(n))_{n=0}^{\infty}$ are $1, 1, 47, 7395, 2453425, 1399055625$. For $n \geq 2$ the following congruence holds:

$$v(n) \equiv -\frac{1}{2} \sum_{m=1}^{n-1} \binom{2n}{2m} v(m) v(n-m).$$

So if we assume that $v(k) \equiv 0$ for $2 \leq k \leq n$, then it is clear that $v(n+1) \equiv 0$, and the lemma follows by induction. □

Remark 2.4.1. Whereas Theorem 2.2.1 is general for all primes, the lemma we just proved was stated for $p = 5$. In fact, experimental evidence suggested that this lemma could be generalized to the statement that $u(n)$ and $v(n)$ are both congruent to 0 mod p for all $n \geq \frac{p+1}{2}$, when p is a prime congruent to 1 mod 4. This observation was subsequently verified in [**Wak20**] and used to give an elementary proof of Romik's conjecture for $p = 4k+1$, expanding on the method used here for $p = 5$.

Proof of Theorem 2.4.1. In view of Lemma 2.4.1, we may restrict the class of partitions that need to be considered in the summation appearing in (2.7). More specifically, let $\mathcal{P}^3_{n,k} \subset \mathcal{P}'_{n,k}$ be the set of partitions of n into k parts among the first three odd positive integers, $1, 3, 5$. Since $u(n)$ vanishes mod 5 for $n > 2$, and therefore $u\left(\frac{i-1}{2}\right)$ vanishes mod 5 for $i > 5$, summands in (2.7) that are indexed by partitions not in $\mathcal{P}^3_{2n,2k}$ have a residue of 0 mod 5. Thus we obtain an equivalent definition of $s(n,k)_5$ to that in (2.7) if we replace the indexing set with $\mathcal{P}^3_{2n,2k}$ and adopt the convention that $s(n,k)_5 = 0$ for pairs (n,k) such that $\mathcal{P}^3_{2n,2k}$ is empty.

Furthermore, for $n = 0, 1, 2$, $u(n) \equiv 1$. Hence, $u\left(\frac{i-1}{2}\right) \equiv 1$ for $i = 1, 3, 5$, and if we substitute these values of $u\left(\frac{i-1}{2}\right)_5$ into (2.7), we obtain

$$s(n,k)_5 = \sum_{\lambda \in \mathcal{P}^3_{2n,2k}} \left[\frac{(2n)!}{c_1!3!^{c_3}c_3!5!^{c_5}c_5!}\right]_5, \tag{2.10}$$

with the convention that $s(n,k)_5 = 0$ if $\mathcal{P}^3_{2n,2k} = \emptyset$. The expression is already interesting. One immediate implication is that if $5k < n$, then $r(n,k)_5 = s(n,k)_5 = 0$, since $\mathcal{P}^3_{2n,2k}$ is clearly empty (see Figure 1).

To reduce the sum in (2.10) further, we recall that in the field of residues modulo 5 nonzero elements are invertible; therefore, since we've shown that each summand in (2.10) is an integer, we can replace 3! in the denominator with 1 and replace $5! = 5 \cdot 4!$ with $5 \cdot (-1)$ without changing the value of the summand's residue mod 5. Thus, we have

$$s(n,k)_5 = \sum_{\lambda \in P^3_{2n,2k}} \left[\frac{(2n)!(-1)^{c_5}}{c_1!c_3!c_5!}\right]_5. \tag{2.11}$$

Next, identify elements of $P^3_{2n,2k}$ in the obvious way with triples (c_1, c_3, c_5) of non-negative integers satisfying the pair of equations

$$\begin{cases} \sum_{i=1}^3 ic_i & = 2n \\ \sum_{i=1}^3 c_i & = 2k. \end{cases}$$

For a given pair (n,k), if we fix c_5 to be some integer c, then this becomes an invertible linear system with

$$c_1 = 3k - n + c, \quad c_3 = n - k - 2c.$$

There exists $(c_1, c_3, c) \in P^3_{2n,2k}$ satisfying the system if and only if $n \le 5k$ and

$$\max(0, n - 3k) \le c \le \left\lfloor \frac{n-k}{2} \right\rfloor.$$

This allows us to rewrite (2.11) as a summation over a single index parameter:

$$s(n,k)_5 = \begin{cases} \sum_{c=\max(0,n-3k)}^{\lfloor \frac{n-k}{2} \rfloor} \left[\frac{(2n)!(-1)^c}{(3k-n+c)!(n-k-2c)!c!5^c}\right]_5 & \text{if } n \leq 5k \\ 0 & \text{if } n > 5k. \end{cases} \tag{2.12}$$

Our next step in the proof is to simplify (2.12) further by showing that the summation depends only on the term corresponding to the largest value of the index parameter, namely $c = \lfloor \frac{n-k}{2} \rfloor$, because all other terms are divisible by 5. This will be the content of Lemma 2.4.2 below. The proof of the lemma will use the following formula of Legendre [**Leg08**], which we record here as a theorem. For p a prime number and n a positive integer, let $\omega_p(n)$ denote the p-adic valuation of n (meaning that $\omega_p(n)$ is the largest natural number α such that p^α divides n), and let $s_p(n)$ denote the sum of the digits in the base-p expansion of n.

THEOREM 2.4.2 (Legendre).

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

LEMMA 2.4.2. *For integers $0 < k \leq n \leq 5k$, the quantity*

$$V(c) := \omega_5\left(\frac{(2n)!(-1)^c}{(3k-n+c)!(n-k-2c)!c!5^c}\right),$$

as a function of $c \in \mathbb{Z}$, is minimized over $max(0, n-3k) \leq c \leq \lfloor \frac{n-k}{2} \rfloor$ when $c = \lfloor \frac{n-k}{2} \rfloor$ and for no other values of c.

PROOF. Assume $k+1 < n < 5k-1$, as otherwise there is nothing to check. Let $c \in \{\max(0, n-3k), \cdots, \lfloor \frac{n-k}{2} \rfloor - 1\}$, and let $\delta = \lfloor \frac{n-k}{2} \rfloor - c > 0$. Then,

$$\begin{aligned} V(c) - V\left(\left\lfloor \frac{n-k}{2} \right\rfloor\right) &= V(c) - V(c+\delta) = \omega_5((3k-n+c+\delta)!) - \omega_5((3k-n+c)!) \\ &+ \omega_5((n-k-2(c+\delta))!) - \omega_5((n-k-2c)!) \\ &+ \omega_5((c+\delta)!) - \omega_5(c!) \\ &+ \omega_5(5^{c+\delta}) - \omega_5(5^c). \end{aligned} \tag{2.13}$$

Each line of the summation contains a difference that we would like to estimate from below. To do that, we note the general fact that if a and b are positive integers, then the estimate $\omega_5((a+b)!) - \omega_5(a!) \geq \omega_5(b!)$ follows from

$$\omega_5((a+b)!) = \omega_5(a!) + \omega_5(b!) + \omega_5\left(\binom{a+b}{a}\right).$$

We also note that $n-k-2(c+\delta) = n-k-2\lfloor \frac{n-k}{2} \rfloor \in \{0,1\}$ and $n-k-2c \in \{2\delta, 2\delta+1\}$. Therefore, we can bound from below each line in (2.13) to obtain the estimate

$$V(c) - V\left(\left\lfloor \frac{n-k}{2} \right\rfloor\right) \geq 2\omega_5(\delta!) - \omega_5((2\delta+1)!) + \delta.$$

An application of Theorem 2.4.2 now yields

$$\begin{aligned} V(c) - V\left(\left\lfloor \frac{n-k}{2} \right\rfloor\right) &\geq 2\frac{\delta - s_5(\delta)}{4} - \frac{2\delta+1-s_5(2\delta+1)}{4} + \delta \\ &= \delta - \frac{s_5(\delta)}{2} + \frac{1}{4}(s_5(2\delta+1) - 1) \\ &> \delta - s_5(\delta) \\ &\geq 0, \end{aligned}$$

where the last two inequalities amount to the simple fact that for p prime, any integer $k > 1$ satisfies $1 < s_p(k) \leq k$. We have shown that $V(c)$ assumes its smallest value uniquely at $c = \lfloor \frac{n-k}{2} \rfloor$. $\square$

Proof of Theorem 2.4.1, continued. By the lemma, all of the summands in (2.12), except the one indexed by $c = \lfloor \frac{n-k}{2} \rfloor$, must vanish mod 5, since they have positive valuation. The remaining summand may or may not vanish. In any case, we have the following simplified formula for $s(n,k)_5$, $1 \leq k \leq n \leq 5k$.

$$s(n,k) \equiv \begin{cases} \dfrac{(2n)!(-1)^{\frac{n-k}{2}}}{\left(\frac{5k-n}{2}\right)!\left(\frac{n-k}{2}\right)!5^{\frac{n-k}{2}}} & \text{if } n-k \text{ is even} \\[2ex] \dfrac{(2n)!(-1)^{\frac{n-k-1}{2}}}{\left(\frac{5k-n-1}{2}\right)!\left(\frac{n-k-1}{2}\right)!5^{\frac{n-k-1}{2}}} & \text{if } n-k \text{ is odd} \end{cases} \tag{2.14}$$

Now we want to translate this into a formula for $r(n,k)_5 = 2_5^{n-k}s(n,k)_5$. The congruence of $(n-k)$ modulo 4 determines the congruence of 2^{n-k} modulo 5, as well as the sign of $(-1)^{\frac{n-k}{2}}$ (respectively $(-1)^{\frac{n-k-1}{2}}$) in the case $n-k$ is even (respectively odd). However, it turns out that we need only consider parity, since $2^{n-k}(-1)^{\frac{n-k}{2}} \equiv 1$, if $n-k$ is even, and $2^{n-k}(-1)^{\frac{n-k-1}{2}} \equiv 2$, if $n-k$ is odd. Combined with (2.14) this completes the proof of Theorem 2.4.1. $\square$

2.4.2. Proof of Theorem 1.2.1 (ii). Now that we have a nice expression for $r(n,k)_5$, we return to the main objective of this section, proving Theorem 1.2.1 (ii).

LEMMA 2.4.3. *In order to prove Theorem 1.2.1 (ii), it suffices to prove the following: For $n \geq 3$,*

$$\sum_{\substack{\frac{n}{5} \leq k \leq n \\ k \text{ even}}} r(n,k) \equiv \sum_{\substack{\frac{n}{5} \leq k \leq n \\ k \text{ odd}}} r(n,k) \equiv 0. \tag{2.15}$$

PROOF. Assume that (2.15) holds. Then

$$\sum_{\frac{n}{5} \leq k \leq n} r(n,k)(-1)^k = \sum_{\substack{\frac{n}{5} \leq k \leq n \\ k \text{ even}}} r(n,k) - \sum_{\substack{\frac{n}{5} \leq k \leq n \\ k \text{ odd}}} r(n,k) \equiv 0.$$

Subtracting $r(n,n)(-1)^n$ from the left and right sides we obtain

$$\sum_{\frac{n}{5} \leq k \leq n-1} r(n,k)(-1)^k \equiv r(n,n)(-1)^{n+1}. \tag{2.16}$$

A quick application of Theorem 2.4.1 shows that $r(n,n) \equiv 1$ for all n (in fact, it's not hard to deduce from (2.3) and the fact that $u(1) = 1$ that $r(n,n) = 1$ for all n), and we have also observed above that $r(n,k) \equiv 0$ when $5k < n$. Therefore, from (2.16) we obtain

$$\sum_{k=1}^{n-1} r(n,k)(-1)^k \equiv (-1)^{n+1}. \tag{2.17}$$

Now we prove by induction that $d(n) \equiv (-1)^{n+1}$ for $n \geq 1$. The cases $n = 1$ and $n = 2$ can be checked directly, since $d(1) = -1$ and $d(2) = 51$. Also from (2.4) and Lemma 2.4.1, we see that when $n \geq 3$, the following holds:

$$d(n) \equiv -\sum_{k=1}^{n-1} r(n,k)d(k).$$

Thus, if $n \geq 3$ and we assume the induction hypothesis that $d(k) \equiv (-1)^{k+1}$ for all $1 \leq k < n$, it follows that

$$d(n) \equiv -\sum_{k=1}^{n-1} r(n,k)(-1)^{k+1} \equiv \sum_{k=1}^{n-1} r(n,k)(-1)^k.$$

But the right-hand-side is congruent mod 5 to $(-1)^{n+1}$, by (2.17). This verifies the induction step. Thus, the truth of (2.15) implies that of Theorem 1.2.1 (ii). $\square$

We will now use some concepts from group theory to verify that (2.15) holds. For n a positive integer, let S_n denote the symmetric group on n letters, and recall that every element of S_n has a unique decomposition as a product of disjoint cycles. Let X_n be the set of elements $x \in S_n$ such that $x^5 = 1$. For any non-negative integer $k \leq n$, let X_n^k denote the set of elements $x \in S_n$ such that x can be written as a disjoint product of k five-cycles and $n - 5k$ one-cycles. Then

$$X_n = \bigcup_{k=0}^{\lfloor \frac{n}{5} \rfloor} X_n^k \, . \tag{2.18}$$

The connection to Theorem 2.4.1 is the following lemma.

Lemma 2.4.4. *For $n > 3$,*

(i)
$$|X_{2n}| = \sum_{\substack{\frac{n}{5} \leq k \leq n \\ n-k \text{ even}}} \frac{(2n)!}{\left(\frac{5k-n}{2}\right)! \left(\frac{n-k}{2}\right)! 5^{\frac{n-k}{2}}} \, ,$$

(ii)
$$2(2n)(2n-1)(2n-2) \cdot |X_{2n-3}| = \sum_{\substack{\frac{n}{5} \leq k < n \\ n-k \text{ odd}}} \frac{2(2n)!}{\left(\frac{5k-n-1}{2}\right)! \left(\frac{n-k-1}{2}\right)! 5^{\frac{n-k-1}{2}}} \, .$$

Proof. Fix $n > 3$. For each k, $0 \leq k \leq n$, it is not hard to show that X_n^k is a conjugacy class in S_n with cardinality

$$|X_n^k| = \frac{n!}{(n-5k)!k!5^k}$$

(see e.g. [**DF04**, Prop. 11 and Exercise 33 in Sec. 4.3]). From (2.18),

$$|X_{2n}| = \sum_{0 \leq k \leq \frac{2n}{5}} |X_{2n}^k| = \sum_{0 \leq k \leq \frac{2n}{5}} \frac{(2n)!}{(2n-5k)!k!5^k}.$$

Therefore, to prove part (i) of the lemma, we must show that the quantity $\frac{n-k}{2}$ assumes every value in the set $T_1 = \{0, 1, \ldots, \lfloor \frac{2n}{5} \rfloor\}$ exactly once as k ranges over the set $T_2 = \{k : \lceil \frac{n}{5} \rceil \leq k \leq n, \, n-k \text{ even}\}$. This is not hard to see, since the change of variable $k \mapsto \frac{n-k}{2}$ maps n to 0, and is linear with first difference $-1/2$, while both T_1 and T_2 have the same cardinality, as one can deduce from a simple analysis of the cases of the congruence modulo 5 of n.

Similarly,

$$|X_{2n-3}| = \sum_{0\le k\le \frac{2n-3}{5}} |X_{2n-3}^k| = \sum_{0\le k\le \frac{2n-3}{5}} \frac{(2n-3)!}{(2n-3-5k)!k!5^k},$$

so to prove part (ii) we must show that the quantity $\frac{n-k-1}{2}$ assumes every value in the set $\{0, 1, \dots, \lfloor\frac{2n-3}{5}\rfloor\}$ exactly once as k ranges over $\{k : \lceil\frac{n}{5}\rceil \le k \le n-1,\ n-k \text{ odd}\}$. This can be deduced from the change of variables $k \mapsto \frac{n-k-1}{2}$ and the same type of argument as before. $\square$

Lemma 2.4.4 and Theorem 2.4.1 together imply that if $n > 3$ is even, then $|X_{2n}| \equiv \sum_{\substack{\frac{n}{5}\le k\le n \\ k \text{ even}}} r(n,k)$, and an integer multiple of $|X_{2n-3}|$ is congruent mod 5 to $\sum_{\substack{\frac{n}{5}\le k\le n \\ k \text{ odd}}} r(n,k)$. Therefore, in order to verify that (2.15) holds for $n > 3$ even, it suffices to show that $|X_{2n}| \equiv |X_{2n-3}| \equiv 0$. We have occasion now to inject a dose of algebraic combinatorics into our elementary number theory, as the desired congruence follows from a classical theorem of Frobenius (see e.g. [**Fin78**]).

THEOREM 2.4.3 (Frobenius). *Let G be a finite group whose order is divisible by a positive integer m. Then m divides the cardinality of the set of solutions x in G to the equation $x^m = 1$.*

Since X_n is precisely the set of solutions to the equation $x^5 = 1$ in S_n, the theorem implies that $|X_{2n}| \equiv |X_{2n-3}| \equiv 0$ for even $n > 3$.

Similarly, if $n > 3$ is odd, then $|X_{2n}| \equiv \sum_{\substack{\frac{n}{5}\le k\le n \\ k \text{ odd}}} r(n,k)$, and an integer multiple of $|X_{2n-3}|$ is congruent mod 5 to $\sum_{\substack{\frac{n}{5}\le k\le n \\ k \text{ even}}} r(n,k)$, and we again apply Theorem 2.4.3 to verify (2.15). Finally, if $n = 3$ we can check the validity of (2.15) by directly computing from (2.9) that $r(3,1) \equiv 4, r(3,2) \equiv 0$, and $r(3,3) \equiv 1$. This verifies (2.15) for all $n \ge 3$ and finishes the proof of Theorem 1.2.1 (ii).

2.5. Proof of Theorem 1.2.1 (iii): Vanishing of $d(n)$ modulo $p \equiv 3 \pmod 4$

Throughout this section, we a prime p congruent to 3 modulo 4. Define the constant $n_0 := \frac{p^2-1}{2}$. The notation $A \equiv B$ will be shorthand for $A \equiv B \pmod p$.

2.5.1. A vanishing theorem for $u(n)$ and $v(n)$. We begin with a theorem about the congruences of $(u(n))$ and $(v(n))$ modulo p, similar to Lemma 2.4.1 above.

THEOREM 2.5.1. *The sequences* $(u(n))_{n=0}^{\infty}$ *and* $(v(n))_{n=0}^{\infty}$ *satisfy*

(i)

$$u\left(\frac{p-1}{2}\right) \equiv 0,$$

(ii)

$$u(n) \equiv 0 \text{ for } n \geq n_0,$$

(iii)

$$v(n) \equiv 0 \text{ for } n > n_0.$$

We first deduce a simple lemma that will be used repeatedly, and then we prove the theorem in three parts.

LEMMA 2.5.1. *If* $a, b \in \mathbb{Z}$ *and* $p^2 \leq a < b + p^2 < 2p^2$, *then* $\binom{a}{b} \equiv 0$.

PROOF. The hypothesis implies that $b \leq p^2 - 1$ and $a - b \leq p^2 - 1$. It follows that

$$\omega_p(b!(a-b)!) = \left\lfloor \frac{b}{p} \right\rfloor + \left\lfloor \frac{a-b}{p} \right\rfloor \leq \frac{a}{p}.$$

Meanwhile, since $a \geq p^2$

$$\omega_p(a!) \geq \left\lfloor \frac{a}{p} \right\rfloor + 1 > \frac{a}{p},$$

and therefore $\omega_p\left(\binom{a}{b}\right) > 0$. □

PROOF OF THEOREM 2.5.1 (I). By (2.1), we have

$$\begin{aligned} u\left(\frac{p-1}{2}\right) &= (3 \cdot 7 \cdots (2p-3))^2 \\ &- \sum_{m=0}^{\frac{p-1}{2}-1} \binom{p}{2m+1} \left[1 \cdot 5 \cdots \left(4\left(\frac{p-1}{2} - m\right) - 3\right)\right]^2 u(m). \end{aligned} \tag{2.19}$$

The product $(3 \cdot 7 \cdots (2p-3))^2$ contains as factors all positive integers that are congruent to 3 mod 4 and less than $2p+1$, and p is such a number. Furthermore $\binom{p}{m} \equiv 0$ for $1 \leq m < p$, so the sum in (2.19) also vanishes mod p. □

PROOF OF THEOREM 2.5.1 (II). Set $n_1 = \frac{3(p+1)}{4} < n_0$. Referring to (2.1), observe that we have $3 \cdot 7 \cdots (4n-1))^2 \equiv 0$ for $n \geq \frac{p+1}{4}$, so in particular for $n \geq n_0$. Observe also that $0 \equiv$

$1 \cdot 5 \cdots (4(n-m)-3)$ if $n-m \geq n_1$. It follows that if $n \geq n_0$, we have the following truncated summation for $u(n)$:

$$u(n) \equiv \sum_{m=n-n_1+1}^{n-1} \binom{2n+1}{2m+1} (1 \cdot 5 \cdots (4(n-m)-3))^2 u(m). \tag{2.20}$$

We will also use the fact that

$$\binom{2n+1}{2m+1} \equiv 0 \tag{2.21}$$

for $n_0 \leq n \leq n_0+n_1-2$ and $n_0-n_1+1 \leq m \leq n_0-1$, which follows from Lemma 2.5.1. Indeed, the assumptions on n in (2.21) imply that

$$p^2 = 2n_0+1 \leq 2n+1 \leq 2n_0+2n_1-3 \leq 2p^2-2,$$

and hence

$$p^2 + \frac{3}{2}(p+1) + 2 = 2n_0 - 2n_1 + 3 \leq 2m+1 \leq 2n_0 - 1 = p^2 - 2.$$

But $p^2 + \frac{3}{2}(p+1) + 2 \geq (2n+1) - p^2 + 1$, for $n \leq n_0 + n_1 - 2$. In brief, Lemma 2.5.1 applies with $a = 2n+1$ and $b = 2m+1$, verifying (2.21).

It follows that $u(n_0) \equiv 0$, since (2.21) implies that all of the binomial coefficients in (2.20) vanish mod p when $n = n_0$. Now suppose that

$$u(n_0) \equiv u(n_0+1) \equiv \cdots \equiv u(n_0+k-1) \equiv 0,$$

for some k such that $1 \leq k \leq n_1 - 2$. This supposition, along with (2.20), implies that

$$\begin{aligned} u(n_0+k) &\equiv \sum_{m=n_0+k-n_1+1}^{n_0+k-1} \Bigg[\binom{2(n_0+k)+1}{2m+1} \\ &\qquad \times (1 \cdot 5 \cdots (4(n_0+k-m)-3))^2 u(m) \Bigg] \\ &\equiv \sum_{m=n_0+k-n_1+1}^{n_0-1} \Bigg[\binom{2(n_0+k)+1}{2m+1} \\ &\qquad \times (1 \cdot 5 \cdots (4(n_0+k-m)-3))^2 u(m) \Bigg]. \end{aligned}$$

By (2.21) all the binomial coefficients in the sum vanish; hence $u(n_0+k) \equiv 0$. Since k was arbitrary, we can conclude that $u(n) \equiv 0$ when $n_0 \leq n \leq n_0 + n_1 - 2$.

Finally, by (2.20) $u(n)_p$ is a sum involving only those values of u evaluated at integers in $[n - n_1 + 1, n - 1]$; if these values of u vanish mod p, then so does $u(n)$. Therefore, if one can show that $u(n)$ vanishes mod p for $n_1 - 1$ consecutive values of n, then by induction $u(n)$ must vanish mod p for all larger n. But we've already shown above that $u(n)$ vanishes for $n \in [n_0, n_0 + n_1 - 2]$, so it follows that $u(n)$ vanishes for all $n \geq n_0$. □

Proof of Theorem 2.5.1 (iii). Referring to the recursive definition for $v(n)$ in (2.2), observe that $1 \cdot 5 \cdots (4n-3) \equiv 0$ for $n \geq \frac{3p+3}{4}$ and hence for $n \geq n_0$. Furthermore, if $n = n_0 + 1$ and $1 \leq m \leq n_0$, then Lemma 2.5.1 applies with $a = 2n$ and $b = 2m$ and hence $\binom{2n}{2m} \equiv 0$. Therefore, $v(n_0 + 1) \equiv 0$.

Now let $n > n_0$ be arbitrary, and assume as an induction hypothesis that $v(k) \equiv 0$ for all $n_0 < k < n$. Then

$$v(n) \equiv -\frac{1}{2} \sum_{m=1}^{n-1} \binom{2n}{2m} v(m) v(n-m). \tag{2.22}$$

If $n \geq 2n_0$, then $n - m > n_0$ for all values of the summation index m, so by the induction hypothesis $v(n-m)$ vanishes mod p and so does the sum. So assume that $n \leq 2n_0$. Then we may restrict the sum in (2.22) to index values $m \in [n - n_0, n_0]$, since for other values of m either $m > n_0$ or $n - m > n_0$. However, for any such m, we can apply Lemma 2.5.1 with $a = 2n$ and $b = 2m$, since $p^2 \leq 2n$ and $2n - p^2 + 1 \leq 2m \leq 2n_0 = p^2 - 1$. It follows that every binomial coefficient in (2.22) vanishes mod p and so does $v(n)$. Induction on $n > n_0$ completes the proof. □

2.5.2. Proof of Theorem 1.2.1 (iii). We begin with a fact similar to Lemma 2.4.3, in that it shifts the burden of proof entirely to the array $(r(n,k))$.

Lemma 2.5.2. *If $r(n,k) \equiv 0$ for all pairs (n,k) such that $1 \leq k \leq n_0 < n$, then Theorem 1.2.1 (iii) is true.*

Figure 2 below gives an illustration of the lemma's hypothesis in the case $p = 7$.

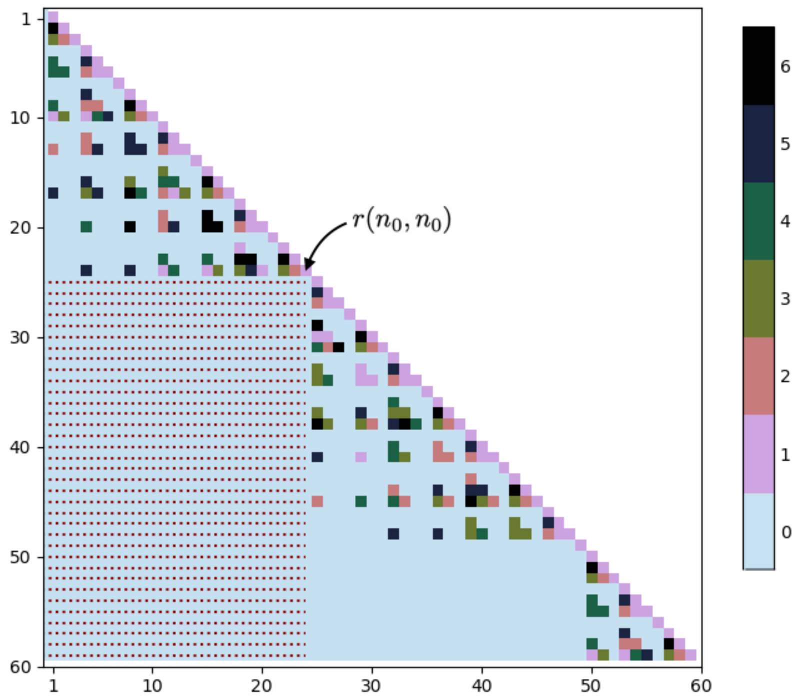


FIGURE 2.2. Congruences of $r(n,k)$ mod 7, $1 \leq k \leq n < 60$. The rows are indexed by n, and the colors indicate residue classes of $r(n,k)$ mod 7, according to the colorbar. Note that $n_0 = \frac{p^2-1}{2} = 24$ for $p = 7$. The submatrix $(r(n,k))_{1 \leq k \leq n_0 < n}$, where $r(n,k)$ vanishes by Theorem 2.5.2, is emphasized.

PROOF. Equation (2.4) and Theorem 2.5.1 imply that if $n > n_0$ then

$$d(n) \equiv -\sum_{k=1}^{n-1} r(n,k)d(k).$$

If we assume the hypothesis of the lemma, then

$$d(n_0+1) \equiv -\sum_{k=1}^{n_0} r(n_0+1,k)d(k) \equiv 0,$$

since all the summands vanish mod p. Moreover for general $n > n_0$,

$$d(n+1) \equiv -\sum_{k=n_0+1}^{n} r(n,k)d(k).$$

Therefore, if we assume that $d(k) \equiv 0$ for all k such that $n_0+1 \leq k \leq n$, then $d(n+1) \equiv 0$. It follows by induction that $d(n) \equiv 0$ for all $n > n_0$, which is the statement of Theorem 1.2.1 (iii). $\square$

As we did in Section 2.4, for $p = 5$, we would now like to restrict the class of partitions that we need to consider in (2.7), for $p \equiv 3 \pmod 4$. Let $\mathcal{P}^*_{2n,2k} \subset \mathcal{P}'_{2n,2k}$ denote the set of partitions λ whose parts are all less than p^2, and such that no part of λ is equal to p, i.e. $c_p = 0$ and $c_i = 0$ for $i \geq p^2$. Theorem 2.5.1 implies that we may replace the index set in the summation (2.7) with $\mathcal{P}^*_{2n,2k}$, since any partition $\lambda \in \mathcal{P}'_{2n,2k} \setminus \mathcal{P}^*_{2n,2k}$ must contain a part λ_i such that $u\left(\frac{\lambda_i - 1}{2}\right)_p = 0$ and hence will contribute 0 to the sum. In other words,

$$s(n,k)_p = \sum_{\lambda \in \mathcal{P}^*_{2n,2k}} \left((N_\lambda)_p \prod_{i=1}^{2n} \left[u\left(\frac{i-1}{2}\right)^{c_i} \right]_p \right), \tag{2.23}$$

with the convention that $s(n,k)_p = 0$ if $\mathcal{P}^*_{2n,2k} = \emptyset$. The key to using formula (2.23) is the following theorem.

Theorem 2.5.2. *Let $(n,k) \in \mathbb{N}^2$ be such that $1 \leq k \leq n_0 < n$. Then*

$$\omega_p(N_\lambda) > 0. \tag{2.24}$$

The theorem implies, by (2.23), that $r(n,k) = 2^{n-k}s(n,k)$ vanishes mod p for $1 \leq k \leq n_0 < n$, and in view of Lemma 2.5.2 will complete the proof of Theorem 1.2.1 (iii).

We record as a lemma a few very basic facts about arithmetic that we will use freely in the proof of Theorem 2.5.2 to bound various quanitites. Recall that $s_p(n)$ denotes the sum of the base-p digits in a positive integer n.

Lemma 2.5.3. *If x and y are positive integers with base-p expansions $x = \sum_{i\geq 0} x_i p^i$ and $y = \sum_{i \geq 0} y_i p^i$, then*

(i) $s_p(x+y) \leq s_p(x) + s_p(y)$, *with equality if and only if there are no carries when x is added to y in base p, if and only if $x_i + y_i \leq p - 1$ for all i.*

(ii) $s_p(px) = s_p(x)$.

(iii) $s_p(x) = x$ *if and only if* $x \leq p - 1$.

Proof of Theorem 2.5.2. Suppose $\lambda \in \mathcal{P}^*_{2n,2k}$. Then

$$c(\lambda) = (c_1, c_2, \ldots, c_{2n}) = (c_1, c_2, \ldots c_{p-1}, 0, c_{p+1}, \ldots c_{p^2-1}, 0 \ldots 0).$$

For each i with $1 \leq i < p^2$ we define numbers a_0^i and a_1^i so that $c_i = a_0^i + a_1^i p$ is the base-p expansion of c_i, where the exponents serve as indices, and there are at most two non-zero digits in the expansion since $c_i \leq 2k < p^2$. Also for $1 \leq i < p^2$, define b_0^i and b_1^i so that $i = b_0^i + b_1^i p$ is the base-p expansion of i.

By Theorem 2.4.2,

$$\begin{aligned}\omega_p(N_\lambda)(p-1) &= \omega_p\left(\frac{(2n)!}{\prod_{i=1}^{2n} i!^{c_i} c_i!}\right)(p-1) \\ &= 2n - s_p(2n) - \sum_{i=1}^{2n}[c_i(i - s_p(i)) + (c_i - s_p(c_i))] \,.\end{aligned}$$

The latter summation can be restricted to index values $i \in [1, p^2)$, since $c_i = 0$ for $i \geq p^2$. Thus we have

$$\begin{aligned}\omega_p(N_\lambda)(p-1) &= 2n - s_p(2n) - \sum_{i=1}^{p^2-1}[c_i(i - s_p(i)) + (c_i - s_p(c_i))] \\ &= \left[\sum_{i=1}^{p^2-1} s_p(i)c_i\right] + \left[\sum_{i=1}^{p^2-1}(s_p(c_i) - c_i)\right] - s_p(2n) \,,\end{aligned}$$

where the last equality just amounts to cancelling the terms $2n$ and $-2n = -\sum_{i=1}^{p^2-1} ic_i$. We expand all the terms in the last line base-p, obtaining

$$\omega_p\left(N_\lambda\right)(p-1) = \left[\sum_{i=1}^{p^2-1}(b_0^i + b_1^i)(a_0^i + a_1^i p)\right] + \left[\sum_{i=1}^{p^2-1} a_1^i(1-p)\right] - s_p\left(\sum_{i=1}^{p^2-1}(b_0^i + b_1^i p)(a_0^i + a_1^i p)\right) \,. \tag{2.25}$$

Now we regroup terms in the right-hand side of the latter equation and apply Lemma 2.5.3, writing

$$
\begin{aligned}
\omega_p\left(N_\lambda\right)(p-1) = &\left[\sum_{i=1}^{p^2-1}(b_0^i+b_1^i)a_1^ip\right]+\left[\sum_{i=1}^{p^2-1}(b_0^i+b_1^i)a_0^i\right]+\left[\sum_{i=1}^{p^2-1}a_1^i(1-p)\right] \\
&-s_p\left(\sum_{i=1}^{p^2-1}(b_0^i+b_1^ip)a_0^i+\sum_{j=1}^{p^2-1}(b_0^j+b_1^jp)a_1^jp\right) \qquad (2.26)\\
\geq &\left[\sum_{i=1}^{p^2-1}(b_0^i+b_1^i)a_1^ip\right]-s_p\left(\sum_{i=1}^{p^2-1}(b_0^i+b_1^ip)a_1^ip\right)+\left[\sum_{i=1}^{p^2-1}a_1^i(1-p)\right] \qquad (2.27)\\
&+\left[\sum_{i=1}^{p^2-1}(b_0^i+b_1^i)a_0^i\right]-s_p\left(\sum_{i=1}^{p^2-1}(b_0^i+b_1^ip)a_0^i\right) \qquad (2.28)\\
\geq &\ 0,
\end{aligned}
$$

where we justify the last inequality as follows. The quantity in (2.28) is non-negative by Lemma 2.5.3, and we claim that the quantity in (2.27) is also non-negative. To show that, write the quantity as

$$
\left\{\left[\sum_{i=1}^{p^2-1}(b_0^i+b_1^i)a_1^i\right]-s_p\left(\sum_{i=1}^{p^2-1}(b_0^i+b_1^ip)a_1^ip\right)\right\}
$$

$$
+\left\{\left[\sum_{i=1}^{p^2-1}(b_0^i+b_1^i)a_1^i(p-1)\right]+\left[\sum_{i=1}^{p^2-1}a_1^i(1-p)\right]\right\}.
$$

The first bracketed term is non-negative by Lemma 2.5.3, and the second bracketed term is non-negative since $b_0^i+b_1^i\geq 1$ for all i.

Suppose now that $\omega_p(N_\lambda)=0$. Then the inequality that we used to transition from (2.26) to (2.27) and (2.28) must be an equality, and the quantity in (2.28) and the bracketed quantities above must all vanish. These facts have a number of consequences. First, in the second bracketed quantity, since $b_0^i+b_1^i\geq 1$ for all i, we have $a_1^i(b_0^i+b_1^i)\geq a_1^i$ for all i. This implies that $a_1^i=0$, or $(b_0,b_1)=(1,0)$, or $(b_0,b_1)=(0,1)$. Since no part of λ is equal to p, by the definition of $\mathcal{P}^*_{2n,2k}$, the last option is only possible if $a_1^i=0$. We conclude that $a_1^i=0$ for all $i\geq 2$. In view of this, the identity

$$s_p\left(\sum_{i=1}^{p^2-1}(b_0^i+b_1^ip)a_0^i+\sum_{j=1}^{p^2-1}(b_0^j+b_1^jp)a_1^jp\right)$$
$$=s_p\left(\sum_{i=1}^{p^2-1}(b_0^i+b_1^ip)a_0^i\right)+s_p\left(\sum_{i=1}^{p^2-1}(b_0^i+b_1^ip)a_1^ip\right)$$

(from the transition from (2.26) to (2.27) and (2.28)), can be simplified to

$$s_p\left(\left[\sum_{i=1}^{p^2-1}(b_0^i+b_1^ip)a_0^i\right]+a_1^1p\right)=s_p\left(\sum_{i=1}^{p^2-1}(b_0^i+b_1^ip)a_0^i\right)+a_1^1. \tag{2.29}$$

Furthermore, the fact that the quantity in (2.28) vanishes implies that (2.29) can be written as

$$s_p\left(\left[\sum_{i=1}^{p^2-1}(b_0^i+b_1^ip)a_0^i\right]+a_1^1p\right)=\left[\sum_{i=1}^{p^2-1}(b_0^i+b_1^i)a_0^i\right]+a_1^1. \tag{2.30}$$

We can estimate the left-hand side of (2.30) by

$$\begin{aligned}s_p\left(\left[\sum_{i=1}^{p^2-1}(b_0^i+b_1^ip)a_0^i\right]+a_1^1p\right)&\le s_p\left(\sum_{i=1}^{p^2-1}b_0^ia_0^i\right)+s_p\left(p\left[\sum_{i=1}^{p^2-1}b_1^ia_0^i\right]+a_1^1p\right)\\&=s_p\left(\sum_{i=1}^{p^2-1}b_0^ia_0^i\right)+s_p\left(\left[\sum_{i=1}^{p^2-1}b_1^ia_0^i\right]+a_1^1\right)\\&\le\left[\sum_{i=1}^{p^2-1}b_0^ia_0^i\right]+\left[\sum_{i=1}^{p^2-1}b_1^ia_0^i\right]+a_1^1,\end{aligned} \tag{2.31}$$

which is just the right-hand side of (2.30), we must have equality throughout (2.31). It follows that

$$s_p\left(\sum_{i=1}^{p^2-1}b_0^ia_0^i\right)+s_p\left(\left[\sum_{i=1}^{p^2-1}b_1^ia_0^i\right]+a_1^1\right)=\left[\sum_{i=1}^{p^2-1}b_0^ia_0^i\right]+\left[\sum_{i=1}^{p^2-1}b_1^ia_0^i\right]+a_1^1,$$

and hence, by Lemma 2.5.3 (iii), we see that

$$\left[\sum_{i=1}^{p^2-1}b_0^ia_0^i\right]\le p-1\,,\quad\text{and}\quad\left[\sum_{i=1}^{p^2-1}b_1^ia_0^i\right]+a_1^1\le p-1. \tag{2.32}$$

Recalling that $2n = \sum_{i=1}^{p^2-1} ic_i$, and that $a_1^i = 0$ for all $i \geq 2$, we see from (2.32) that

$$\begin{aligned}
2n &= a_1^1 p + \sum_{i=1}^{p^2-1} (b_0^i + b_1^i p) a_0^i \\
&= \left[\sum_{i=1}^{p^2-1} b_0^i a_0^i\right] + p\left(\left[\sum_{i=1}^{p^2-1} b_1^i a_0^i\right] + a_1^1\right) \\
&\leq (p-1) + p(p-1) \\
&= p^2 - 1.
\end{aligned}$$

In conclusion, the supposition above that $\omega_p(N_\lambda) = 0$ led us to the statement that $2n \leq p^2 - 1$, or equivalently $n \leq n_0$. Since the hypothesis of Theorem 2.5.2 assumes $n > n_0$, we have proved the theorem's contrapositive. $\square$

2.6. Concluding remarks

Remark 2.6.1. Theorem 2.5.2 was custom-made to use in conjunction with Lemma 2.5.2. However, the odd parity of the parts in $P^*_{2n,2k}$ was never used in the proof, nor was the congruence of p modulo 4, nor were the even parity of the number of parts ($2k$) or the value ($2n$) of the integer to which they summed. In fact, the reader will see that the same proof goes through to verify the following general combinatorial result.

Theorem 2.6.1. *Let $p > 0$ be a prime number. Let $(n, k) \in \mathbb{N}^2$ be such that $1 \leq k < p^2 \leq n$, and let λ be a partition of n into k parts such that all the parts are less than p^2 and no part is equal to p. Then p divides N_λ.*

As our proof is elementary number theoretic, it would be interesting to give a combinatorial proof or an algebraic proof of this theorem. We leave as an open problem the challenge of doing so. We also pose the problem of generalizing to the higher-power case, where $1 \leq k < p^\alpha \leq n$ for $\alpha > 2$, e.g. by finding appropriate restrictions on the parts in λ to ensure that N_λ is divisible by $p^{\alpha-1}$.

Remark 2.6.2. The inspiration for our proof of Theorem 1.2.1 (iii) was supplied by Figure 2, from which it seems obvious that $s(n, k)$ vanishes modulo p for $1 \leq k \leq n_0 < n$, at least in the case $p = 7$. It is natural then to ask why the results for $p = 5$ and $p = 4k + 3$ are so different. Surely the difference should be reflected somewhere in the proofs of the respective statements. The most important difference is that $u(2)_5 = u\left(\frac{5-1}{2}\right)_5 = 1$, whereas $u\left(\frac{p-1}{2}\right)_p = 0$ for $p = 4k + 3$. Consequently, there exist partitions in $\mathcal{P}^3_{2n,2k}$ that index non-vanishing summands in (2.7), and indeed those partitions with the largest possible number of 5's are the important ones. On the other hand, when $p = 4k + 3$, partitions in $\mathcal{P}'_{2n,2k}$ with parts equal to p do not contribute to the sum in (2.7) at all. It seems plausible then that a statement similar to Theorem 2.5.1 that is general for powers p^α of primes $p = 4k + 3$ would exist and be useful in conjunction with a higher-power version of Theorem 2.6.1 in proving that $d(n)$ eventually vanishes modulo p^α.

CHAPTER 3

Residual functions for shape summation of the weight-2 Eisenstein series and the Weierstrass $\wp$-function

We continue from Section 1.3, where we defined the notion of shape summation and stated our main result, Theorem 1.3.1. This chapter is organized as follows. In **Section** 3.1 we give the proof of Theorem 1.3.1. In **Section** 3.1 we discuss shape summation for the Weierstrass $\wp$-function and prove Theorem 1.3.2. In **Section** 3.2 we demonstrate our notion of residual function with some concrete examples, and in **Section** 3.3 we make some concluding remarks.

3.1. Proof of Theorems 1.3.1 and 1.3.2: K-summation of G_2 and $\wp$

A key ingredient in the proof is the following Lemma 3.1.1, which shows that the right-hand side of (1.14) is the K-summation of a different series than (1.13), which has the advantage of being a telescoping series in the summation index n. In proving Theorem 1.3.1, we will use this series to write $G_2(\tau)$ as a series that converges absolutely, which will allow us to compare it with $G_2(K,\tau)$ and show that the series in Lemma 3.1.1 coincides with the residual function $E(K,\tau)$.

Lemma 3.1.1. *Let $K \in \mathcal{K}$ be a shape with corresponding function h_K, supported on $[-A,A]$. Then*

$$\sum_K \left(\frac{1}{m\tau+n} - \frac{1}{m\tau+n+1}\right) = 4\int_0^A \frac{h_K(x)}{\tau^2x^2 - h_K^2(x)}\,dx,$$

where we exclude summands corresponding to $m=0$, that is, we set $a_{0,n}=0$ for all n in (1.12).

Proof. For brevity of notation, we set $h = h_K$ for the rest of the proof. To evaluate the sum in the lemma, we rewrite it as

(3.1)
$$\sum_K \left(\frac{1}{m\tau+n} - \frac{1}{m\tau+n+1}\right) = \lim_{\lambda\to\infty} \sum_{\substack{-\lambda A\le m\le \lambda A\\ m\neq 0}} \sum_{-\lambda h(m/\lambda)\le n\le \lambda h(m/\lambda)} \left(\frac{1}{m\tau+n} - \frac{1}{m\tau+n+1}\right).$$

After telescoping the inner summation, this becomes

$$\lim_{\lambda\to\infty} \sum_{\substack{-\lambda A\le m\le\lambda A\\ m\ne 0}} \left(\frac{1}{m\tau-\lfloor\lambda h(\frac{m}{\lambda})\rfloor} - \frac{1}{m\tau+\lfloor\lambda h(\frac{m}{\lambda})\rfloor} + \frac{1}{m\tau+\lfloor\lambda h(\frac{m}{\lambda})\rfloor} - \frac{1}{m\tau+\lfloor\lambda h(\frac{m}{\lambda})\rfloor+1}\right)$$
$$= \lim_{\lambda\to\infty} \sum_{\substack{-\lambda A\le m\le\lambda A\\ m\ne 0}} \left[\left(\frac{2\lfloor\lambda h(\frac{m}{\lambda})\rfloor}{m^2\tau^2-\lfloor\lambda h(\frac{m}{\lambda})\rfloor^2}\right) + \frac{1}{(m\tau+\lfloor\lambda h(\frac{m}{\lambda})\rfloor)(m\tau+\lfloor\lambda h(\frac{m}{\lambda})\rfloor+1)}\right]$$
$$= 2\lim_{\lambda\to\infty} \sum_{1\le m\le\lambda A} \left(\frac{2\lfloor\lambda h(\frac{m}{\lambda})\rfloor}{m^2\tau^2-\lfloor\lambda h(\frac{m}{\lambda})\rfloor^2}\right)$$
$$= 4\lim_{\lambda\to\infty} \frac{1}{\lambda} \sum_{1\le m\le\lambda A} \left(\frac{\lambda^{-1}\lfloor\lambda h(\frac{m}{\lambda})\rfloor}{\lambda^{-2}m^2\tau^2-\lambda^{-2}\lfloor\lambda h(\frac{m}{\lambda})\rfloor^2}\right).$$

Since, $\lambda^{-1}\lfloor\lambda h(\frac{m}{\lambda})\rfloor \sim h(\frac{m}{\lambda})$ and $\lambda^{-2}\lfloor\lambda h(\frac{m}{\lambda})\rfloor^2 \sim h(\frac{m}{\lambda})^2$ as $\lambda\to\infty$, the above limit is the same as the limit of a Riemann sum,

$$4\lim_{\lambda\to\infty} \frac{1}{\lambda} \sum_{1\le m\le\lambda A} \left(\frac{h(\frac{m}{\lambda})}{\lambda^{-2}m^2\tau^2-h^2(\frac{m}{\lambda})}\right),$$

which is the integral in the lemma. □

We now observe that

$$\sum_{m\ne 0}\left[\sum_{n\in\mathbb{Z}}\left(\frac{1}{m\tau+n}-\frac{1}{m\tau+n+1}\right)\right]=0.$$

To see this, note that for any $m\ne 0$, the inner sum converges absolutely (since the summands are $O(1/n^2)$ as $n\to\infty$), and is equal to

$$\lim_{N\to\infty}\sum_{n=-N}^{N-1}\left(\frac{1}{m\tau+n}-\frac{1}{m\tau+n+1}\right)=\lim_{N\to\infty}\left(\frac{1}{m\tau-N}-\frac{1}{m\tau+N}\right)=0.$$

Thus, we can write $G_2(\tau)$ in a different form, namely

$$G_2(\tau)-\sum_{n\ne 0}\frac{1}{n^2} = \sum_{m\ne 0}\left[\sum_{n\in\mathbb{Z}}\frac{1}{(n+m\tau)^2}\right]$$
$$= \sum_{m\ne 0}\left[\sum_{n\in\mathbb{Z}}\frac{1}{(n+m\tau)^2}\right] - \sum_{m\ne 0}\left[\sum_{n\in\mathbb{Z}}\left(\frac{1}{m\tau+n}-\frac{1}{m\tau+n+1}\right)\right]$$
$$= \sum_{m\ne 0}\left[\sum_{n\in\mathbb{Z}}\frac{1}{(m\tau+n)^2(m\tau+n+1)}\right].$$

The latter series has the advantage of converging absolutely by comparison with $\sum_m \sum_n \frac{1}{(m\tau+n)^3}$ (see Lemma 1.1 in [2]).

Next we observe, still setting $h = h_K$, that Definition 1.3.3 can be expressed as

$$G(K,\tau) = \sum_{n\neq 0} \frac{1}{n^2} + \lim_{\lambda\to\infty} \sum_{\substack{-\lambda A\leq m\leq \lambda A \\ m\neq 0}} \sum_{-\lambda h(m/\lambda)\leq n\leq \lambda h(m/\lambda)} \frac{1}{(m\tau+n)^2}. \tag{3.2}$$

By combining (3.1) and (3.2) , we obtain

$$\begin{aligned}
&G_2(K,\tau) - \sum_{n\neq 0}\frac{1}{n^2} - \sum_K \left(\frac{1}{m\tau+n} - \frac{1}{m\tau+n+1}\right) \\
&= \lim_{\lambda\to\infty} \sum_{\substack{-\lambda A\leq m\leq \lambda A \\ m\neq 0}} \sum_{-\lambda h(m/\lambda)\leq n\leq \lambda h(m/\lambda)} \left(\frac{1}{(m\tau+n)^2} - \frac{1}{m\tau+n} + \frac{1}{m\tau+n+1}\right) \\
&= \lim_{\lambda\to\infty} \left[\sum_{\substack{-\lambda A\leq m\leq \lambda A \\ m\neq 0}} \sum_{-\lambda h(m/\lambda)\leq n\leq \lambda h(m/\lambda)} \frac{1}{(m\tau+n)^2(m\tau+n+1)}\right] \\
&= \sum_{m\neq 0}\left[\sum_{n\in\mathbb{Z}} \frac{1}{(m\tau+n)^2(m\tau+n+1)}\right],
\end{aligned}$$

where in the last equality we have appealed to absolute convergence to justify rearranging the series. From the above we see that

$$E(K,\tau) = G_2(K,\tau) - G_2(\tau) = \sum_K \left(\frac{1}{m\tau+n} - \frac{1}{m\tau+n+1}\right).$$

When we replace the latter sum with the integral expression from the lemma, the proof of Theorem 1.3.1 is complete. □

We discussed after Definition 1.6 how thinking about elliptic functions and the motivation behind the definition of $\wp$ leads one to consider different orders of summation for the conditionally convergent infinite series $\sum_{m,n} \frac{1}{(z+n+m\tau)^2}$, in a way that is precisely analogous to the situation with G_2. It turns out, as we see in Theorem 1.3.2, that this leads to exactly the same notion of "residual function" that we already defined. As with G_2, the two most obvious orders for summing the series are as iterated summations with respect to the summation indices m, n, in the two possible orders. The comparison between these two orders of summation is given in the following result, which is a more explicit version of a result stated implicitly as part of an exercise on p. 281 of [**SS03**], and is analogous to (1.4).

Proposition 3.1.1. *For $z \notin \mathbb{Z}\tau + \mathbb{Z}$, the following identity holds, where summations are in the indicated order, over all pairs $(m, n) \in \mathbb{Z}^2$.*

$$\sum_m \left[\sum_n \frac{1}{(z+n+m\tau)^2} \right] = \sum_n \left[\sum_m \frac{1}{(z+n+m\tau)^2} \right] + \frac{2\pi i}{\tau}.$$

Proof. We rewrite the sum defining $\wp(z)$ in the following way, excluding from the summations the terms corresponding to $m = n = 0$.

$$\begin{aligned}
\wp(z) &= \frac{1}{z^2} + \sum_m \left[\sum_n \left(\frac{1}{(z+n+m\tau)^2} - \frac{1}{(m\tau+n)^2} \right) \right] \\
&= \frac{1}{z^2} + \sum_m \left[\sum_n \frac{1}{(z+n+m\tau)^2} \right] - \sum_m \left[\sum_n \frac{1}{(m\tau+n)^2} \right] \\
&= \frac{1}{z^2} + \sum_m \left[\sum_n \frac{1}{(z+n+m\tau)^2} \right] - G_2(\tau).
\end{aligned}$$

Meanwhile, we can sum the function $\wp(z)$ in the reverse order, by absolute convergence, obtaining

$$\begin{aligned}
\wp(z) &= \frac{1}{z^2} + \sum_n \left[\sum_m \left(\frac{1}{(z+n+m\tau)^2} - \frac{1}{(m\tau+n)^2} \right) \right] \\
&= \frac{1}{z^2} + \sum_n \left[\sum_m \frac{1}{(z+n+m\tau)^2} \right] - \sum_n \left[\sum_m \frac{1}{(m\tau+n)^2} \right] \\
&= \frac{1}{z^2} + \sum_n \left[\sum_m \frac{1}{(z+n+m\tau)^2} \right] - G_2(\tau) + \frac{2\pi i}{\tau},
\end{aligned}$$

by (1.4). The proposition follows by comparing these two expressions for $G_2(\tau)$. $\square$

Recall that in Chapter 1 we defined general shape summation for the series associated with the $\wp$-function by

$$\wp(K, z) := \sum_K \frac{1}{(z+n+m\tau)^2} \qquad (z \notin \mathbb{Z}\tau + \mathbb{Z}),$$

for $K \in \mathcal{K}$ and $\tau \in \mathbb{H}$. We prove Theorem 1.3.2 now, which asserted the identity

$$\wp(K, z) = \wp(z) + G_2(\tau) + E(K, \tau).$$

Proof of Theorem 1.3.2. By absolute convergence of the sum defining $\wp(z)$, we can sum over the integer lattice points in any order without changing the function's value. Therefore,

$$\wp(z) = \sum_K \left[\frac{1}{(z+n+m\tau)^2} - \frac{1}{(n+m\tau)^2} \right],$$

where $a_{0,0} = \frac{1}{z^2}$ in (1.12). Thus,

$$\begin{aligned}
\wp(z) &= \sum_K \frac{1}{(z+n+m\tau)^2} - \sum_K \frac{1}{(n+m\tau)^2} \\
&= \wp(K,z) - G_2(K,\tau) \\
&= \wp(K,z) - (G_2(\tau) + E(K,\tau)).
\end{aligned}$$

□

3.2. Examples

The integral in the explicit formula (1.14) can sometimes be evaluated in closed form. Here are a few examples.

(1) **Rectangle.** As we saw in Section 1.3.2, the residual function for the rectangle $[-c,c]\times[-1,1]$ with aspect ratio $c>0$ is $E(K,\tau) = -\frac{4}{\tau}\tanh^{-1}(c\tau)$.

(2) **Disk.** When K is the disk of radius 1 centered at the origin, we have $h_K(x) = \sqrt{1-x^2}$, $x\in[-1,1]$. According to Theorem 1.3.1, we have

$$E(K,\tau) = 4\int_0^1 \frac{\sqrt{1-x^2}}{\tau^2x^2-(1-x^2)}\,dx = \frac{-2\pi i}{\tau+i}.$$

(3) **Diamond.** For the last example we let K be the diamond $\{x+iy : |x|+|y|\le 1\}$. Then $h_K(x) = 1-|x|$, $x\in[-1,1]$. We have

$$E(K,\tau) = 4\int_0^1 \frac{1-x}{\tau^2x^2-(1-x)^2}\,dx = \frac{4\log(-i\tau)+2\pi i\tau}{1-\tau^2},$$

where log denotes the principal branch of the logarithm.

3.3. Concluding Remarks

(1) We have constructed a large family of examples of natural rearrangements of conditionally convergent series. Our explicit formula (1.14) for the residual function $E(K,\tau)$ provides a

general way to evaluate the discrepancy between any rearrangement in the family we considered and the "default" ordering of the series, thus generalizing the well-known relation (1.4) and its equivalent version (1.5). As we mentioned before, this quasimodularity relation (1.5), while being an example of "bad behavior" from the point of view of infinite series, is actually a useful and important property of G_2, forming the basis for the study of many of its properties as well as the properties of additional functions in complex analysis and the theory of modular forms that are constructed using G_2 as a building block. In view of the importance of (1.5), it is interesting to wonder whether (1.14) might similarly provide fresh insight into some questions about modular forms that are of independent interest.

(2) Also related to (1.5) is the observation that for any $K \in \mathcal{K}$, if K is symmetric about the line $y = x$, then the residual function $E(K, \tau)$ satisfies a similar functional equation, namely

$$E(K, \tau) = \tau^{-2} E(K, -1/\tau) - \frac{2\pi i}{\tau}, \tag{3.3}$$

which differs from the equation for $G_2(\tau)$ only in the sign of the $\frac{2\pi i}{\tau}$ term. This can be derived as follows. Given a shape K, we let K^T be the shape obtained by reflecting K about the line $x = y$.

Replacing τ with $-1/\tau$ in the K-summation of $G_2(K, \tau)$, one obtains

$$\begin{aligned} G(K, -1/\tau) &= \tau^2 G(K^T, \tau) \\ &= \tau^2 (G_2(\tau) + E(K^T, \tau)). \end{aligned}$$

Meanwhile, the functional equation for $G_2(\tau)$ implies that

$$\begin{aligned} G(K, -1/\tau) &= G_2(-1/\tau) + E(K, -1/\tau) \\ &= \tau^2 G_2(\tau) - 2\pi i \tau + E(K, -1/\tau). \end{aligned}$$

Equating these two expressions for $G(K, -1/\tau)$ and subtracting the term $\tau^2 G_2(\tau)$ from both sides gives

$$E(K^T, \tau) = \tau^{-2} E(K, -1/\tau) - \frac{2\pi i}{\tau}.$$

If K is symmetric about $y = x$, then $K^T = K$, so (3.3) holds.

(3) We saw how a shape $K \in \mathcal{K}$ gives rise to residual functions, which are computed as a kind of integral transform of the associated bounding function h_K. It seems natural to try to reverse this correspondence and ask which holomorphic functions $f : \mathbb{H} \to \mathbb{C}$ occur as residual functions for shapes in $\mathcal{K}$. We leave this as an open problem.

(4) Finally, we note that one can consider summation with respect to shapes in greater levels of generality. In particular, one could expand the class of shapes $\mathcal{K}$ by relaxing the symmetry conditions, the condition of compactness, or both. We leave to the interested reader to work out the details of such generalizations.

CHAPTER 4

A criterion for sharpness in tree enumeration and the asymptotic number of triangulations in Kuperberg's G_2 spider

This chapter is organized as follows.

In **Section 4.1** we continue with our discussion from Section 1.4.4 about simply generated trees and identity (1.24) – $y(x) = xA(y(x))$. We state and prove our asymptotic sharpness criterion, Theorem 4.1.3, of which Theorem 1.4.2 is a corollary. We also give a pair of examples.

In **Section 4.2** we prove Kuperberg's conjecture (1.19) way of 1.4.2. As mentioned in Chapter 1, a preliminary step is to obtain a growth estimate for the sequence (b_n). This we do in Proposition 4.2.1 by way of saddle-point analysis of a known formula from the character theory of Lie algebra representations.

In **Section 4.3** we prove the remaining parts of Theorem 1.4.1. The constant ρ is evaluated in Proposition 4.3.1, and the remainder of the section contains a detailed singularity analysis that leads to (1.22) and (1.23). An outline of the method is given at the beginning of the section. We will also obtain along the way another proof of Conjecture 1.4.1 that is independent of the first one in Section 4.2.

In **Section 4.4** we apply the sharpness criterion Theorem 4.1.3 (or Theorem 1.4.2) to the Lie algebra B_2 and the asymptotic counting of the quadrangulations in the B_2 spider.

4.1. Criterion for sharpness

We pick up from Section 1.4.4 and the identity (1.24) – $y(x) = xA(y(x))$. Throughout this chapter, when thinking of power series as analytic functions we will use the variable z or w, e.g. writing $y(z)$. On the other hand, writing $y(x)$ will emphasize thinking of formal power series combinatorially, without considerations of convergence or analytic continuation. This distinction is more psychological than mathematical and could also just be ignored.

4.1.1. Preliminary lemmas.

LEMMA 4.1.1. *Let* $A(x) = 1 + \sum_{i\geq 1} a_i x^i$ *and* $y(x) = \sum_{i\geq 1} y_i x^i$ *be power series over* $\mathbb{R}$ *related by* (1.24)*, with* $a_i \geq 0$ *for all* $i \geq 1$ *. Then* $y_i \geq 0$ *for all* i*. Let* R *be the radius of convergence of* A*, and let* r *denote the radius of convergence of* y*. Then* $R > 0$ *iff* $r > 0$*, and*

$$y(z) = zA(y(z)) \tag{4.1}$$

for $z \in \Omega = \{z \in \mathbb{C} : |z| < r\}$*. Also,* $y(r) \leq R$*, including when* $y(r) = \infty$*.*

REMARK 4.1.1. Notice that neither r nor R are required to be finite in the lemma. However, it is easy to see that if $a_n \geq 1$ for all large enough n, then $R \leq 1$, so that $y(r) \leq 1$ by the lemma, and hence $r < \infty$.

PROOF. Given $A(x)$, the Lagrange Inversion Theorem [**Sta99**, Ch. 5.4] implies that the unique power series solution to (1.24) is given by

$$y_i = \frac{1}{i}[x^{i-1}](A(x)^i), \tag{4.2}$$

for all $i \geq 1$, where $[x^i]f(x)$ denotes the i'th coefficient of a power series $f(x)$. The right-hand side is non-negative, so $y_i \geq 0$ for all i.

To prove the next part, suppose $R > 0$ and consider the function $F(z, w) = w - zA(w)$, which is analytic for $z \in \mathbb{C}$ and $|w| < R$. Then $F_w = 1 - zA'(w)$ is non-zero at $(0, 0)$, so that by the implicit function theorem there exists a function $\tilde{y}$, analytic near the origin, with $F(z, \tilde{y}(z)) = 0$. By (4.2), $\tilde{y} = y$, which shows that $r > 0$.

Now assume $r > 0$ and let z be a non-negative number in Ω. Then

$$zA(y(z)) = z\sum_{i=0}^{\infty}\left[a_i\left(\sum_{j=1}^{\infty} y_j z^j\right)^i\right] = \sum_{i=1}^{\infty}\sum_{j=i}^{\infty}(c_{ij}z^j) = \sum_{j=1}^{\infty}\left[\left(\sum_{i=1}^{j} c_{ij}\right) z^j\right],$$

where $c_{ij} = a_i[x^{j-1}]\left(\sum_{k=1}^{\infty} y_k x^k\right)^i$, and the interchange of the order of summation is permitted since each c_{ij} is non-negative. The fact that $y(z) = \sum_{j=1}^{\infty}\left[\left(\sum_{i=1}^{j} c_{ij}\right) z^j\right]$ is just a reformulation of (1.24). So $zA(y(z)) = y(z) < \infty$. Thus, the double sum above is absolutely convergent on Ω, and (4.1) is valid on Ω.

Next, since the coefficients of $y(x)$ are non-negative, y maps $[0, r)$ bijectively to $[0, y(r))$. Therefore, if $0 < |z| < y(r)$, then $|z| = y(w)$ for some $w \in (0, r)$, and $A(|z|) = y(w)/w < \infty$. So $R \geq y(r)$. In particular $R > 0$, since $y_1 = 1$ and hence $y(r) \geq r$. The lemma is trivial when $r = R = 0$. $\square$

As mentioned in the proof, for a generating function $A(x) = 1+\sum_{n\geq 1} a_n x^n$, the unique solution $y(x)$ to (1.24) is given by formula (4.2). When furthermore the a_n's are non-negative, we associate to A another function ψ, defined by

$$\psi(z) := \frac{z}{A(z)} \tag{4.3}$$

on the set $\{z : |z| < R \text{ and } A(z) \neq 0\}$, where R is the radius of convergence of A. On the same set, we have the identity

$$\psi'(z) = \frac{A(z) - zA'(z)}{A(z)^2} = \frac{1 - \sum_{n=1}^{\infty} a_n(n-1)z^n}{A(z)^2}. \tag{4.4}$$

The key point, explained in the following lemma, is that ψ is the functional inverse of y.

Remark 4.1.2. While an attempt is made in what follows to state results with a certain amount of generality, a good class of generating functions to have in mind is that for which $(a_n)_{n\geq 1}$ is *an eventually positive and increasing sequence of integers*, in which case $(y_n)_{n\geq 1}$ has the same property. This includes the functions from Theorem 1.4.1.

Lemma 4.1.2. *Assume the hypotheses of Lemma 4.1.1, and that $R > 0$. Let $\Omega = \{z \in \mathbb{C} : |z| < r\}$. The function $y : \Omega \to y(\Omega)$ is a biholomorphism, and $\psi(y(z)) = z$ for $z \in \Omega$. In particular, ψ is well-defined and analytic on $y(\Omega)$. Furthermore, if $A(x)$ is not identically equal to 1, then $r < \infty$. Finally, if $y(r) < \infty$, then y extends continuously to the boundary $\partial\Omega$, ψ extends continuously to the boundary of $y(\Omega)$, and $\psi(y(z)) = z$ holds for $z \in \partial\Omega$.*

Proof. Note that $y(0) = 0$, $A(0) = 1$, and A is analytic on $y(\Omega)$ by Lemma 4.1.1. If $y(z) = 0$ for $z \in \Omega$, then by (4.1) we see that

$$z = z \cdot 1 = z \cdot A(y(z)) = y(z) = 0.$$

So y vanishes at the origin and nowhere else in Ω. Therefore, for $z \in \Omega \setminus \{0\}$ we have $A(y(z)) = y(z)/z \neq 0$, and A doesn't vanish on $y(\Omega)$. As a consequence ψ is defined there and analytic, and it follows from (4.1) that $\psi(y(z)) = z$ for $z \in \Omega$. The injectivity of y is now a simple consequence of (4.1). Indeed, if $y(z) = y(w) \neq 0$ for $z, w \in \Omega$, then $z \neq 0$, $w \neq 0$, and

$$zA(y(z)) = y(z) = y(w) = wA(y(w)) = wA(y(z)),$$

so $w = z$.

To see that $r < \infty$ in the case $A(x) \neq 1$, observe that if instead y is entire, i.e. $\Omega = \mathbb{C}$, then $R = \infty$ by Lemma 4.1.1. Moreover, $[0, \infty) = y([0, \infty)) \subset y(\mathbb{C})$, since y generally maps $[0, r)$ onto $[0, y(r))$, as noted in the proof of Lemma 4.1.1. Since A doesn't vanish on $y(\mathbb{C})$, ψ' is defined on a neighborhood of $[0, \infty)$. Also, $a_n > 0$ for some $n > 0$, since $A \neq 1$. It follows then from the series expansion in (4.4) that $\psi'(\tau) = 0$ for some $\tau > 0$. By the inverse function theorem, we have $y'(\psi(\tau)) = 1/\psi'(\tau) = \infty$, which contradicts that y is entire. It follows that r is finite.

To prove the last part, $y(r) < \infty$ implies that $\sum_{n=0}^{\infty} y_n z^n$ converges on $\overline{\Omega}$, and further that this convergence is uniform, by the non-negativity of the y_n and the Weierstrass M-test. This gives the continuous extension of y to $\partial\Omega$. The same argument can be used to show that $A \circ y$ extends continuously to $\partial\Omega$. By continuity, $zA(y(z)) = y(z)$ for $z \in \partial\Omega$, and A doesn't vanish on $\partial(y(\Omega))$ by the same argument as above. So $\psi(y(z)) = z$ for $z \in \partial\Omega$. $\square$

4.1.2. Criterion for sharpness and proof of Theorem 1.4.2. The following proposition provides a way to check that the radius of convergence of the function A in (4.1) is as small as possible, namely equal to $y(r)$. A slight variation of the theorem is converse to a known fact (see Theorem 4.1.2(1) below).

THEOREM 4.1.1. *Suppose that the generating functions $A(x) = 1 + \sum_{n=1}^{\infty} a_n x^n$ and $y(x) = \sum_{n=1}^{\infty} y_n x^n$, with radii of convergence R and r respectively, satisfy the following conditions:*

(1) $R > 0$, and $a_n \geq 0$ for $n \geq 1$.

(2) $A(x)$ and $y(x)$ are related as formal power series by (1.24).

If $y(r) < R \leq \infty$, then $A(z) - zA'(z)$ vanishes at $z = y(r)$.

PROOF. Assume that $y(r) < R$. By Lemma 4.1.2, $r > 0$, and since $y_1 = 1$, r must be finite, as otherwise $y(r) = \infty$. To prove the theorem, we will show that the further assumption that $A(z) - zA'(z) \neq 0$ for $z = y(r)$ leads to a contradiction of the fact that r is the radius of convergence of y.

Assume that $A(y(r)) - y(r)A'(y(r)) \neq 0$. Recall the function ψ, defined in (4.3) by $\psi(z) = z/A(z)$. By Lemma 4.1.2, ψ is analytic and equal to y^{-1} on $y(\Omega)$, where $\Omega = \{z \in \mathbb{C} : |z| < r\}$. We claim that there exists a small open disk E centered at $y(r)$, such that ψ extends to be analytic on $y(\Omega) \cup E$. Indeed, since $y(r) < R$, it follows that A is analytic on an open disk, which we call E, that is centered at $y(r)$ and contained in the disk $\{z : |z| < R\}$. Also, since A is continuous and $A(y(r)) = y(r)/r > 0$, we may assume, by possibly replacing E with a smaller open disk, that A does not vanish on E. It follows that ψ is analytic on $y(\Omega) \cup E$, as the reciprocal of a non-vanishing analytic function, and furthermore (4.4) holds on $y(\Omega) \cup E$. By (4.4), the assumption that $A(y(r)) - y(r)A'(y(r)) \neq 0$ implies that $\psi'(y(r)) \neq 0$. It follows that ψ is locally invertible at $y(r)$. That is, after possibly replacing E with a smaller open disk centered at $y(r)$, we see that the map $\psi|_E : E \to \psi(E)$ is a homeomorphism, with an analytic inverse map $\psi|_E^{-1}$. Since r is a boundary point of Ω, we have by Lemma 4.1.2 that $\emptyset \neq \psi(y(\Omega) \cap E) \subset \Omega \cap \psi(E)$. Since $\psi|_E$ is injective, one sees that y and $\psi|_E^{-1}$ agree on the open set $\psi(y(\Omega) \cap E)$. By uniqueness of analytic continuation $\psi|_E^{-1}$ also agrees with y on the larger open set $\Omega \cap \psi(E)$, thus acting as an analytic continuation of y to $\psi(E)$. Since $r \in \psi(E)$, this contradicts a fact known as Pringsheim's Theorem [**Hil59**, Thm. 5.7.1], which asserts that an analytic function with non-negative real coefficients and a finite radius of convergence necessarily has a singularity at the point where the boundary of its disk of convergence intersects $[0, \infty)$. This is the contradiction we sought, and the proof is complete. $\square$

If we phrase the theorem in a slightly weaker form by replacing the consequent with the statement that $A(z) - zA'(z) = 0$ for *some* z in $(0, R)$, then the converse is well-known to be true, and it follows from Theorem 4.1.2(1) below. Theorem 4.1.2 contains even deeper asymptotic information than that, however, in particular regarding the *subexponential* (i.e. polynomial) growth rate of (y_n). This, it turns out, will be instrumental in proving Theorem 1.4.1, as it shows how information about the growth of (y_n) can certify that $A(z) - zA'(z)$ does not vanish on $(0, R)$, and hence, by Theorem 4.1.1, that $y(r) = R$.

THEOREM 4.1.2 (Meir, Moon, 1978 [**MM78**]). *Suppose that* $A(x) = 1 + \sum_{n=1}^{\infty} a_n x^n$ *and* $y(x) = \sum_{n=1}^{\infty} y_n x^n$ *(with radii of convergence* R *and* r*, respectively) satisfy conditions (1) and (2) of Theorem 4.1.1. If there exists* $\tau \in (0, R)$*, such that* $A(\tau) - \tau A'(\tau) = 0$*, then*

(1) $y(x)$ has radius of convergence $r = \tau/A(\tau)$, and $y(r) = \tau < R$.

If, in addition, gcd$\{n \geq 1 : a_n > 0\} = 1$, then

(2) the coefficient sequence $(y_n)_{n=1}^{\infty}$ satisfies the following asymptotic estimate: As $n \to \infty$,

$$y_n = \frac{C}{r^n n^{3/2}}(1 + \mathcal{O}(n^{-1})) = \frac{C \cdot A'(\tau)^n}{n^{3/2}}(1 + \mathcal{O}(n^{-1})),$$

where $C = \sqrt{\frac{A(\tau)}{2\pi A''(\tau)}}$.

The theorem's gcd condition is a mild technicality, satisfied for example if (a_n) is eventually increasing. (When the gcd exceeds 1, the asymptotic formula applies with a modified constant C to a subsequence of (y_n).) This theorem appears to have been first established essentially by Meir and Moon in [**MM78**, Thm. 3.1], building on techniques of Darboux [**Dar78**], Pólya [**Pol37**], and others. In [**MM89**] the same authors generalize their analysis to a much broader class of functional equations, of which (1.24) is an example. One may also consult [**Drm04**, Thm. 5] and [**FS09**, Thm. VI.6] for proofs of this more general result, and one may find in [**FS09**, pp. 467-471] a brief note about the theorem's history. Here we only outline the proof.

Proof sketch. To show (1), note that if $A(\tau) - \tau A'(\tau) = 0$ for $\tau \in (0, R)$ and we further assume that $y(r) > \tau$, then since $y(0) = 0 < \tau < y(r)$ and y is increasing on $[0, r)$, there is some point z in $(0, r)$ where y is analytic and $y(z) = \tau$. Since $\psi = y^{-1}$ on $(0, r)$, we see that $0 = \psi'(\tau) = (y'(z))^{-1}$, which is absurd. Next, since $z \mapsto (A(z) - zA'(z))$ is a decreasing function on $(0, R)$, if $y(r) < \tau$, then $\psi'(y(r)) \neq 0$. One can then argue, as in the proof of Theorem 4.1.1, that y admits an analytic continuation to a neighborhood of r. This contradicts Pringsheim's Theorem, establishing that $y(r) = \tau$. To derive (2), the main idea is that under the hypotheses of the theorem the function $\psi - r$ has a second-order zero at τ, which implies that $y - \tau$ behaves locally like a square-root function near r. The Taylor coefficients of such a function are known by the generalized binomial theorem and Theorem 1.4.4 to have a subexponential growth factor of $n^{-3/2}$. □

Combining Theorems 4.1.1 and 4.1.2, we obtain the following dichotomy.

Theorem 4.1.3 (Criterion for sharpness, full version). *Suppose that $A(x)$ and $y(x)$ (with radii of convergence R and r, respectively) satisfy conditions (1) and (2) of Theorem 4.1.1 and the gcd condition of Theorem 4.1.2. Then exactly one of the following is true:*

(1) $A(z) - zA'(z)$ is non-vanishing for $z \in (0, R)$, in which case $R = y(r)$.

(2) $R > y(r) = \tau$, where τ is the unique solution to $A(\tau) - \tau A'(\tau) = 0$ on $(0, R)$, and $y_n = Cr^{-n}n^{-3/2}(1 + o(1))$ as $n \to \infty$, for some constant $C > 0$.

In particular, the absence of the $n^{-3/2}$ factor in the asymptotic expansion of y_n certifies that the inequality $y(r) \leq R$ is actually equality, so Theorem 1.4.2 is an immediate corollary.

REMARK 4.1.3. In the interest of painting a clearer picture of the web of ideas involved here, we remark that there is a *weaker criterion* than Theorem 4.1.3 that can be used to deduce the sharpness $y(r) = R$ (in the notation of Theorem 4.1.1 – where we mean "weaker" in the sense of requiring more knowledge about the growth of (y_n) – but with a proof that is much simpler than evoking Theorem 4.1.2. Specifically, if we know that $y_n = \Theta(r^{-n}n^{-\alpha})$ for some $\alpha \geq 2$, then $y'(r) < \infty$ by comparison with the series $\sum_{n\geq 1} n^{-\alpha+1}$. Now suppose toward showing a contradiction that $y(r) < R$. By Theorem 4.1.1, (4.4), and the fact that $A(y(r)) \neq 0$, we see that $\psi'(y(r)) = 0$. It follows that $y'(z)$ is unbounded as $z \to r$ in $[0, r)$, by the inverse function theorem. This contradicts the summability of $y'(r)$, so $y(r) = R$.

4.1.3. A comment on the universality of $n^{-3/2}$. The factor $n^{-3/2}$ in the sharpness criterion is not an anomaly. It is actually ubiquitous in a large class of structures whose generating functions occur as solutions to polynomial systems satisfying a certain technical axiomatic framework. See "irreducible context-free schemas" and the Drmota-Lalley-Woods (DLW) Theorem in Chapter VII of [**FS09**] for a detailed exposition. Example 1 below is a classic example in the case of a single defining polynomial. As another simple example, the reader can try showing as an exercise that if $A(x)$ is a polynomial with non-negative coefficients (corresponding to simply generated trees for which a finite upper bound exists on the allowable number of children per node), then case (2) of Theorem 4.1.3 occurs.

Universality of subexponential growth factors is a common theme in the schematic approach to generating functions. For example, in [**BD15**, Thm 4.2] the authors generalize the $n^{-3/2}$ factor to generating functions satisfying a broader axiomatic framework, removing from the DLW Theorem the so-called "strong connectivity" condition on the defining polynomials, to show that if $y(x)$ is the solution of such an algebraic system, then the subexpontial growth factor of its coefficients is $n^{-\alpha}$ for α a dyadic rational. They apply this result in a criterion [**BD15**, Prop. 4.4] that shows that certain generating functions that occur in lattice-walk models are not $\mathbb{N}$-algebraic, meaning that they cannot arise as solutions to polynomial systems with positive coefficients (the so called "context-free schema" that describes many naturally-occurring examples). The generating function $B(x)$ studied here contributes another example of a natural lattice-walk generating function with $\alpha \neq 3/2$. It will be shown to be non-algebraic in Corollary 4.3.1.

4.1.4. Examples. We give two examples of Theorem 4.1.3. The first is a classical illustration of case (1), and the second is an original example illustrating the boundary case in the theorem, namely when $A(z) - zA'(z)$ vanishes at $z = R$.

EXAMPLE 4.1.1 (Catalan numbers). Let $A(x) = 1/(1-x)$, with radius of convergence $R = 1$, and let $y(x) = \sum_{n\geq 1} y_n x^n$ satisfy (1.15). Then for $n \geq 1$, $y_{n+1} = \binom{2n}{n}/(n+1)$ is the n'th Catalan number. One way to show this (see e.g. [**Drm04**, pp. 1-4]) is to solve $y(x)^2 - y(x) + x = 0$ for $y(x)$ and then develop a Taylor expansion from the solution

$$y(x) = \frac{1 - \sqrt{1-4x}}{2}.$$

We see that the radius of convergence of $y(x)$ is $r = 1/4$, that $y(r) = 1/2 < R$, and that

$$A(x) - xA'(x) = \frac{1-2x}{(1-x)^2}$$

vanishes at $y(r)$. Thus, the well-known asymptotic formula $y_n \sim \pi^{-1/2} 4^{n-1} n^{-3/2}$, as $n \to \infty$, is a direct application of Theorem 4.1.2 above.

EXAMPLE 4.1.2 (Boundary case). Theorem 4.1.3 suggests the following question: Assuming conditions (1) and (2) of Theorem 4.1.1, if $y_n \sim Cr^{-n}n^{-3/2}$ for a constant C, is the inequality $y(r) \leq R$ necessarily strict? This example shows that the answer is no. Let

$$\begin{aligned} A(x) &= 6x + 2(1-4x)^2 - (1-4x)^{5/2} \\ &= 1 + 2x^2 + 20x^3 + 10x^4 + 12x^5 + 20x^6 + \cdots, \end{aligned}$$

where the radical is in terms of the principal logarithm. Then $A(x)$ has radius of convergence $R = 1/4$, and the Taylor coefficients of $(1-4x)^{5/2} = \sum_{n=0}^{\infty} x^n (-4)^n \binom{5/2}{n}$ are easily seen to be integers (the coefficients of $(1-4x)^{1/2}$ are integers in the previous example), and are negative except for the constant term. Let $y(x)$ be the unique solution to (1.24) (e.g. as determined by Lagrange Inversion (4.2)), with radius of convergence r, to be determined. Then one sees that the conditions of Theorem 4.1.1 are met.

Observe that $A(z)-zA'(z)\neq 0$ for $z\in(0,R)$, so Theorem 4.1.3(1) implies that $y(r)=R=1/4$, and also note that $\lim_{z\to R}[A(z)-zA'(z)]=0$, so this is a boundary case. Define $\psi(z)=z/A(z)$ for $|z|<R$ and $A(z)\neq 0$. By Lemma 4.1.2, the identity $z=\psi(y(z))$ remains valid at $z=r$, so

$$r=\psi(R)=\psi(1/4)=1/6.$$

We observe that

$$\frac{1}{6}-\psi(z)=\frac{2(1-4z)^2-(1-4z)^{5/2}}{6A(z)}=(1-4z)^2H(z), \tag{4.5}$$

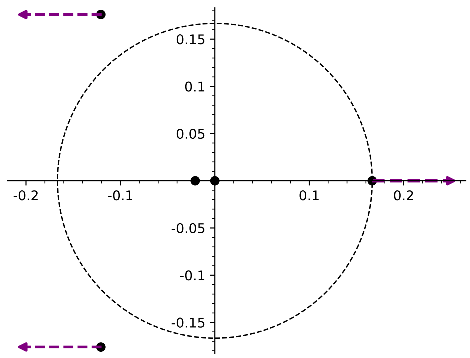
where $H(z)$ is analytic and non-vanishing on a neighborhood of $R=1/4$ in the slit plane $\mathbb{C}\setminus[1/4,\infty)$, and $\lim_{z\to 1/4}H(z)=2/9$.

Now we derive asymptotics for the coefficient sequence (y_n) by using Theorem 1.4.4. To initiate this process we must justify that the function y admits an analytic continuation to a Delta-domain. We will use the fact that A and y are algebraic. Let

$$f(y,z)=1024z^2y^5-256z^2y^4+68z^2y^2-64zy^3-20z^2y+20zy^2+3z^2-4zy+y^2\,.$$

Then one may check that $f(y,\psi(y))=0$ for all y where $\psi(y)$ is defined and non-zero, so in particular on the open set $\{y:|y|<R,y\neq 0\}$. It follows that the function y, defined initially on $\Omega=\{z:|z|<1/6\}$ by the power series above and being inverse to ψ near 0, is an analytic solution to $f(y(z),z)=0$ on Ω. Furthermore, f is analytic on $\mathbb{C}\times(\mathbb{C}\setminus\{0\})$, and the critical points of f (points where both f and $\frac{\partial f}{\partial y}$ vanish) can be computed as the roots of the discriminant of f with respect to y [**Lan02**, Ch. IV, Sec 8]. Using SAGE, we find that the discriminant has roots at $z=0$, $z=1/6$, $z\approx -0.02$, as well as two complex conjugate roots $z\approx -0.12\pm 0.18i$ of modulus larger than $1/6$. As an algebraic function, y extends analytically to any simply-connected domain $\tilde{\Omega}\supset\Omega$ with the following properties: the coefficients of the minimal polynomial of $y(z)$ over $\mathbb{C}(z)$ are analytic (in this case the minimal polynomial is $f(y,z)/1024z^2$), and $\tilde{\Omega}$ contains no roots of the discriminant of f [**Smi59**, p.119]. Furthermore, $f(y(z),z)=0$ for all $\tilde{\Omega}$. An example of such a domain is depicted in Figure 4.1. In particular y extends to a Delta-domain.

FIGURE 4.1. The boundary of the disk Ω and branch cuts whose complement $\tilde{\Omega}$ is a domain of analytic continuation for y and contains a Delta-domain around Ω. Roots of the discriminant of f are also shown.



We claim moreover that $y(z) \notin \mathbb{C} \setminus [1/4, \infty)$ for $z \in \tilde{\Omega}$. Indeed, if we view $f(y, z)$ as quadratic over z, and collect the coefficients in $\mathbb{C}[y]$ to write $f(y, z) = a(y)z^2 + b(y)z + c(y)$, then $f(y, z)$ has discriminant

$$\operatorname{disc}(y) = -\frac{1}{4}(4y-1)^7 - \frac{1}{2}(4y-1)^6 - \frac{1}{4}(4y-1)^5,$$

making it clear that $f(1/4, z)$ has a unique root of $1/6$ and that for $y > 1/4$, $f(y, z)$ has two complex conjugate roots z and $\bar{z}$. Moreover, one can compute that

$$\begin{aligned} |z|^2 - \frac{1}{36} &= \frac{b(y)^2 + \operatorname{disc}(y)}{4a(y)^2} - \frac{1}{36} = \frac{9b(y)^2 + 9\operatorname{disc}(y) - a(y)^2}{36a(y)^2} \\ &= \frac{-(4y-1)^{10} - 8(4y-1)^9 - \cdots - \frac{81}{2}(4y-1)^3 - \frac{27}{2}(4y-1)^2}{36(4y-1)^{10} + 288(4y-1)^9 + \cdots + \frac{4131}{2}(4y-1)^2 + \frac{2916}{4}(4y-1) + \frac{729}{4}}, \end{aligned}$$

i.e. the non-zero Taylor coefficients of the numerator and denominator are all negative and all positive, respectively. This implies that for $y > 1/4$, one has $|z| < 1/6$. But we know on the other hand that $|y(z)| < 1/4$ for $|z| < 1/6$ – by the non-negativity of (y_n), the fact that $y(1/6) = 1/4$, and the triangle inequality. These two facts imply, since $f(y(z), z) = 0$ for all $z \in \tilde{\Omega}$, that $y(z) \notin [1/4, \infty)$ for $z \in \tilde{\Omega}$. In other words, the values of y on $\tilde{\Omega}$ avoid the branch cut $[1/4, \infty)$.

As a result, we may substitute $y(z)$ for z in (4.5), apply the identity $\psi(y(z)) = z$, and solve for $y(z)$. We find that

$$y(z) - \frac{1}{4} = -\frac{1}{4(H(y(z)))^{1/2}} \left(\frac{1}{6} - z\right)^{1/2},$$

for $z \in \tilde{\Omega}$. It follows that

$$y(z) - \frac{1}{4} \sim \frac{-3}{4\sqrt{2}} \left(\frac{1}{6} - z \right)^{1/2},$$

as $z \to 1/6$ in $\tilde{\Omega}$. We conclude by Theorem 1.4.4 that

$$y_n \sim \frac{K \cdot 6^n}{n^{3/2}},$$

as $n \to \infty$, where $K = \frac{\sqrt{3}}{16\sqrt{\pi}}$.

REMARK 4.1.4. Although (4.2) provides a way to compute (y_n) exactly from $A(x)$, it does not make it easy to determine the asymptotic growth of (y_n) in Example 4.1.2. For this the transfer method was necessary. An interesting feature of this example is the extra labor we must go through to justify that y extends to a Delta-domain. This is due to having equality in the universal estimate $y(r) \leq R$. Indeed, when $y(r) < R$, A and ψ are a priori analytic in a neighborhood of $y(r)$, and this makes the extension of y easier to argue in the majority of applications of the transfer theorems in the literature, e.g. Example 1.4.1. One may also look at the details of Example 4.1.1 for more information about this typical setup. As with Example 4.1.2, our main object of study (Kuperberg's generating function for triangulation counts) contributes a new instance of the atypical setup, $y(r) = R$, as well as ad hoc arguments to justify Delta-domain continuation based on idiosyncrasies of the functions at hand (see Section 4.3).

4.2. Proof of Kuperberg's Conjecture 1.4.1

For the rest of this paper, the generating functions $A(x)$ and $B(x)$ will be those from Theorem 1.4.1. Recall that $1/7$ is the radius of convergence of $B(x)$ and $y(x)$ and that $\rho = 7/B(1/7) = 1/y(1/7)$, and let R denote the radius of convergence of $A(x)$.

It is clear from the definition that $(a_n)_{n\geq 1}$ is an increasing sequence, since given any triangulation of an n-gon ($n \geq 3$) one can add another vertex to obtain a triangulated $(n+1)$-gon without introducing any new internal vertices. So Theorem 1.4.2 applies.

4.2.1. Outline of the proof.

4.2.1. Outline of the proof. Our proof of (1.19) proceeds by the following steps.

(1) With K as in Theorem 1.4.1, we show in Proposition 4.2.1 that as $n \to \infty$,

$$b_n \sim K \frac{7^n}{n^7}.$$

(2) The asymptotic estimate in the previous step, specifically the presence of the n^7 polynomial factor as opposed to a factor of $n^{3/2}$, indicates by Theorem 1.4.2 (or Theorem 4.1.3) that $R = 1/\rho$.

(3) It follows that

$$\limsup_{n\to\infty} \sqrt[n]{a_n} = \rho\,.$$

Observe that $a_{n+m-2} \geq a_n a_m$, for $n, m \geq 2$, since one can always obtain a triangulated $(n+m-2)$-gon by gluing together a triangulated n-gon and a triangulated m-gon along a common edge, and this process does not introduce any new internal vertices. Thus we obtain, for $n, m \geq 2$,

$$\log a_n + \log a_m \leq \log a_{n+m-2} \leq \log a_{n+m}.$$

So $(\log a_n)_{n\geq 2}$ is a superadditive sequence, which implies by a lemma generally attributed to Fekete [**Fek23**] that

$$\lim_{n\to\infty} \sqrt[n]{a_n} = \sup_{n\in\mathbb{N}} \sqrt[n]{a_n}.$$

From the lim sup above, this limit must be ρ. (1.19) then follows directly.

4.2.2. Asymptotics of (b_n). In view of the proof overview from above, the following proposition completes the proof of (1.19). Let K be as defined in Theorem 1.4.1.

PROPOSITION 4.2.1. *As $n \to \infty$, the sequence $(b_n)_{n=0}^{\infty}$ satisfies $b_n \sim K(7^n/n^7)$.*

In the introduction we described a lattice walk model in which the b_n's denote the number of n-step excursions that start and end at the origin. This interpretation suggests that a local central limit theorem will apply for the return probabilities of random paths of length n. A difficulty is that the constraints on allowable steps imply that they are not i.i.d. Luckily, there is a reflection trick due essentially to [**GZ92**] which allows one to express the return probabilities as local linear combinations of the probabilities that *unconstrained* walks in the weight lattice $\cong \mathbb{Z}^2$

will end at various nearby points to the origin. Indeed, this method has been applied to derive asymptotic formulas [**TZ04**, Thm. 8] which imply that the sequence $(\dim \mathrm{Inv}_L(V^{\otimes n}))_{n=1}^{\infty}$, where V is any representation of a complex semi-simple Lie algebra L, is asymptotically equivalent to $C\dim(V)^n n^{-\alpha}$, where α is half the dimension of L (in our case $\alpha = 14/2 = 7$), and the constant term C can also be computed but depends on the specific representation. We nonetheless supply a direct proof of Proposition 4.2.1 based on a saddle-point analysis.

Proof. The random walk model and the reflection trick mentioned above are encoded by the following formula from character theory [**Kup94**, p.15]: b_n is the coefficient of $x^n y^n$ in the Laurent polynomial WM^n, where

$$M(x,y) = 1 + x + y + xy + x^2y + xy^2 + (xy)^2,$$

and

$$W(x,y) = x^{-2}y^{-3}(x^2y^3 - xy^3 + x^{-1}y^2 - x^{-2}y + x^{-3}y^{-1} - x^{-3}y^{-2} + x^{-2}y^{-3} - x^{-1}y^{-3} + xy^{-2} - x^2y^{-1} + x^3y - x^3y^2).$$

We define

$$f(x,y) = \log\left(\frac{1}{7}M(x,y)\right) - \log(x) - \log(y).$$

By Cauchy's residue formula for Taylor coefficients, we have

$$\frac{b_n}{7^n} = \frac{1}{(2\pi i)^2}\oint\oint\left[W(z_1,z_2)\cdot\frac{M(z_1,z_2)^n}{7^n}\cdot\frac{1}{(z_1z_2)^{n+1}}\right]dz_1\,dz_2.$$

We use as contours for both integrals the unit circle about the origin, i.e. $z_1 = e^{iu}$ and $z_2 = e^{iv}$, for $-\pi \le u, v \le \pi$. Thus,

$$\frac{b_n}{7^n} = \frac{1}{4\pi^2}\int_{-\pi}^{\pi}\int_{-\pi}^{\pi}\left[W(e^{iu},e^{iv})\cdot\exp\left(nf(e^{iu},e^{iv})\right)\right]du\,dv. \tag{4.6}$$

The function f satisfies $f(1,1) = f_x(1,1) = f_y(1,1) = 0$, and thus we have

$$f(x,y) = \frac{2}{7}(x-1)^2 + \frac{2}{7}(y-1)^2 + \frac{2}{7}(x-1)(y-1) + \mathcal{O}((x-1,y-1)^3),$$

as $(x,y) \to (1,1)$, where the exponent 3 in the last term signifies a multi-index that ranges over all pairs of non-negative integers whose sum is 3. It follows that

$$f(e^{iu}, e^{iv}) = -\frac{2}{7}u^2 - \frac{2}{7}v^2 - \frac{2}{7}uv + \mathcal{O}((u,v)^3),$$

as $(u,v) \to (0,0)$. Now we make an n-dependent change of variables in (4.6), namely $p = \sqrt{n}u$, and $q = \sqrt{n}v$. The integral becomes

$$\frac{4\pi^2 b_n n}{7^n} = \int_{-\sqrt{n}\pi}^{\sqrt{n}\pi}\int_{-\sqrt{n}\pi}^{\sqrt{n}\pi}\left[W\left(e^{ip/\sqrt{n}}, e^{iq/\sqrt{n}}\right)\exp\left(-\frac{2}{7}p^2 - \frac{2}{7}q^2 - \frac{2}{7}pq + \mathcal{O}\left(\frac{(p,q)^3}{\sqrt{n}}\right)\right)\right] dpdq.$$

By standard estimates, which we omit (and which morally relate to the fact that there is a local central limit theorem for a lattice random walk with i.i.d. steps at work), the above integral can be approximated asymptotically by the completed integral over all of $\mathbb{R}^2$, and the contribution of the $\mathcal{O}((p,q)^3/\sqrt{n})$ term is negligible. Moreover, if for each $k \in \mathbb{N}$ we let $T_k(p,q)$ denote the order k Taylor approximation for $(p,q) \mapsto W(e^{ip}, e^{iq})$, then it suffices to consider integrals of the form

$$\int_{-\infty}^{\infty}\int_{-\infty}^{\infty}\left[T_k(pn^{-1/2}, qn^{-1/2}) \cdot \exp\left(-\frac{2}{7}p^2 - \frac{2}{7}q^2 - \frac{2}{7}pq\right)\right].$$

Computing with SAGE, we find that this integral vanishes for $k < 12$, while

$$\begin{aligned}
&\int_{-\infty}^{\infty}\int_{-\infty}^{\infty}\left[T_{12}(pn^{-1/2}, qn^{-1/2}) \cdot \exp\left(-\frac{2}{7}p^2 - \frac{2}{7}q^2 - \frac{2}{7}pq\right)\right] dpdq \\
&= \frac{1}{n^6}\int_{-\infty}^{\infty}\int_{-\infty}^{\infty}\left[T_{12}(p,q) \cdot \exp\left(-\frac{2}{7}p^2 - \frac{2}{7}q^2 - \frac{2}{7}pq\right)\right] dpdq \\
&= \frac{1}{n^6} \cdot \frac{4117715\sqrt{3}}{216}\pi\ .
\end{aligned}$$

In total, we have shown that $\frac{4\pi^2 b_n n}{7^n} \sim \frac{4117715\sqrt{3}}{216n^6}\pi$, as $n \to \infty$, which implies the asserted value of K. □

4.3. Proof of Theorem 1.4.1: Singularity analysis

Now we complete the proof of Theorem 1.4.1, parts (b)–(d). Recall the functions $y(z) = zB(z)$ and $\psi(z) = z/A(z)$ – where A and B be are still the functions from Theorem 1.4.1 – and that

$1/\rho = y(1/7)$. Throughout the sequel we will also use these function names to indicate analytic continuations to larger domains than their original disks of convergence. Here is an outline of the main steps of the proof, with brief descriptions. Each step has its own dedicated subsection below.

(1) **Evaluation of ρ and analytic continuation of B.** We verify (1.20) in Proposition 4.3.1 using the generating function from Theorem 4.3.1 below, and we establish analytic continuation of B to the domain

$$\tilde{\Omega} := \mathbb{C} \setminus \big((\infty, -1/2] \cup [1/7, \infty)\big),$$

which includes in particular a Delta-domain.

(2) **Singular expansion of B and asymptotic formula for (b_n).** In Proposition 4.3.2 we expand B in terms of a logarithm near the singularity $1/7$, and from that we prove (1.21) and (1.22) by the method of asymptotic transfer.

(3) **Analytic continuation of ψ.** We show that ψ extends analytically to a Delta-domain $\Delta_{1/\rho}$, and that $(y \circ \psi)|_{\Delta_{1/\rho}} = \mathrm{Id}\,|_{\Delta_{1/\rho}}$. See Proposition 4.3.3. This serves as the analytic precondition to justify the next step.

(4) **Singular expansion of ψ near the singularity $1/\rho = y(1/7)$.** We use a bootstrapping technique to locally invert y near $1/7$ up to an asymptotically negligible error term and derive a singular expansion of ψ near $1/\rho$. See Proposition 4.3.4.

(5) **Singular expansion of A near the singularity $1/\rho = y(1/7)$.** From the singular expansion of ψ in the previous step, we obtain a singular expansion for A. See Proposition 4.3.5.

(6) **Asymptotic formula for (a_n).** We verify (1.23) by asymptotic transfer.

4.3.1. Evaluation of ρ and analytic continuation of B. In the recent paper [**BTWZ19**, p. 8] is given the following remarkable closed formula for the generating function B in terms of hypergeometric series.

Theorem 4.3.1 (Bostan, Tirrell, Westbury, Zhang, 2019).

$$B(z) = \frac{1}{30z^5}\left[R_1(z) \cdot {}_2F_1\left(\frac{1}{3}, \frac{2}{3}; 2; \phi(z)\right) + R_2(z) \cdot {}_2F_1\left(\frac{2}{3}, \frac{4}{3}; 3; \phi(z)\right) + 5P(z)\right], \tag{4.7}$$

where

$$R_1(z) = (z+1)^2(214z^3+45z^2+60z+5)(z-1)^{-1},$$

$$R_2(z) = 6z^2(z+1)^2(101z^2+74z+5)(z-1)^{-2},$$

$$\phi(z) = 27(z+1)z^2(1-z)^{-3},$$

$$P(z) = 28z^4+66z^3+46z^2+15z+1.$$

We will use this formula as the starting point for analysis in the next section. As a quick application, we obtain the following result, which verifies (1.20).

Proposition 4.3.1.

$$\rho = \frac{5\pi}{8575\pi - 15552\sqrt{3}}.$$

Proof. Evaluating (4.7) at $x = 1/7$, the formula simplifies to

$$B\left(\frac{1}{7}\right) = \frac{7^5}{30}\left[\frac{-55296}{2401}\cdot {}_2F_1\left(\frac{1}{3},\frac{2}{3};2;1\right) + \frac{9216}{2401}\cdot {}_2F_1\left(\frac{2}{3},\frac{4}{3};3;1\right) + \frac{150}{7}\right].$$

It is now a matter of routine calculation to deduce the value in the proposition. One only needs standard facts about the gamma function, namely that $\Gamma(z+1) = z\Gamma(z)$ for $z \notin \mathbb{Z}_{\leq 0}$ and the following, respectively from [**Bai35**, pp. 2-3] and [**SS03**, Ch.8]:

(1)

$$_2F_1(a,b;c;1) = \frac{\Gamma(c)\Gamma(c-a-b)}{\Gamma(c-a)\Gamma(c-b)} \quad (\mathrm{Re}(c) > \mathrm{Re}(a+b)),$$

(2)

$$\Gamma(z)\Gamma(1-z) = \frac{\pi}{\sin(\pi z)} \quad (z \in \mathbb{C}).$$

Using (1) and then (2) we simplify the above expression for $B(1/7)$ and recall that $\rho = 7/B(1/7)$. □

We also obtain the following corollary.

Corollary 4.3.1. *A(z) and B(z) are not algebraic.*

Proof. The fact that B and y are not algebraic follows since π is transcendental. Since being algebraic is preserved under taking functional and multiplicative inverses, we see that A is also not algebraic. Alternatively, if $F(A(z), z) = 0$ for F a bivariate polynomial with integer coefficients, then $F(A(1/\rho), 1/\rho) = 0$, in particular. But this implies that $F(7/\rho, 1/\rho) = 0$, by the functional equation $y(z) = zA(y(z))$, which is impossible since $1/\rho$ is transcendental. $\square$

In deriving formula (4.7), the authors of [**BTWZ19**] demonstrate that B is the solution of a linear differential equation of the form

$$B''' + a_2 B'' + a_1 B' + a_0 B = 0\,,$$

where the coefficients a_i, $i = 0, 1, 2$, are rational functions with poles at $0, -1/2, -1$, and $1/7$. From this fact, as well as the fact that B is expressed on $\Omega = \{z : |z| < 1/7\}$ by a convergent power series (generating function from Theorem 1.4.1) and is visibly analytic near $z = -1$ (by (4.7) and $\phi(-1)) = 0$), the theory of differential equations implies that B can be continued analytically and uniquely along any path avoiding the set $\{-1/2, 1/7\}$ (e.g. [**Smi59**, p.119]). In particular, B has a unique analytic continuation to the simply-connected doubly slit plane

$$\tilde{\Omega} = \mathbb{C} \setminus \big((\infty, -1/2] \cup [1/7, \infty)\big).$$

In particular, B is continuable to a Delta-domain around Ω. In order to apply Theorem 1.4.4 in the we must determine the nature of B near the singularity $1/7$.

4.3.2. Singular expansion of B and asymptotic formula for (b_n). In this section we expand B in terms of a logarithm near the singularity $1/\rho$ and then derive the asymptotic formulas (1.21) and (1.22) by transfer methods. For the rest of Section 4.3, the principal branch of the logarithm is denoted by log.

4.3.2.1. *Singular expansion of B.*

Proposition 4.3.2. *With $Z = 1 - 7z$ and K as in (1.17),*

$$B(z) = p(Z) - \frac{K}{6!} Z^6 \log Z + Z^7 H_2(Z) + Z^7 H_1(Z) \log Z \tag{4.8}$$
$$= p(Z) - \frac{K}{6!} Z^6 \log Z + \mathcal{O}(Z^7 \log Z),$$

as $z \to 1/7$ in $\tilde{\Omega}$, where $H_1(Z)$ and $H_2(Z)$ are power series with positive radii of convergence and non-zero constant terms, and $p(Z)$ is a degree-six polynomial with $p(0) = B(1/7) = 7/\rho$. The error term $Z^7 H_2(Z) + Z^7 H_1(Z) \log Z$ in (4.8) extends analytically to $\tilde{\Omega}$.

To prove the proposition we will appeal to the following analytic continuation (which is distilled from [**Wol20**]) for the ${}_2F_1$ functions appearing in (4.7).

LEMMA 4.3.1. *For constants $a, b \in \mathbb{R}$ and a variable z satisfying $|1 - z| < 1$, we have*

$$ {}_2F_1(a, b; a + b + 1, z) = C_{a,b} + S_{a,b}(z) + \log(1 - z) \cdot T_{a,b}(z), \tag{4.9}$$

with the following definitions:

$$C_{a,b} := \frac{\Gamma(a + b + 1)}{\Gamma(a + 1)\Gamma(b + 1)},$$

$$T_{a,b}(z) := \frac{\Gamma(a + b + 1)}{\Gamma(a)\Gamma(b)} \cdot \left(\sum_{k=0}^{\infty} \left[\frac{(a + 1)_k (b + 1)_k}{k!(k + 1)!} \cdot (1 - z)^{k+1} \right] \right),$$

and

$$S_{a,b}(z) := \frac{\Gamma(a + b + 1)}{\Gamma(a)\Gamma(b)} \cdot \left(\sum_{k=0}^{\infty} \left[\frac{(a + 1)_k (b + 1)_k}{k!(k + n)!} \cdot c_k \cdot (1 - z)^{k+1} \right] \right),$$

where

$$c_k = \psi_0(a + k + 1) + \psi_0(b + k + 1) - \psi_0(k + 1) - \psi_0(k + 2),$$

for the digamma function $\psi_0 = \Gamma'/\Gamma$, and $(q)_k = q(q + 1) \cdots (q + k - 1)$.

PROOF OF PROPOSITION 4.3.2. The second statement regarding analyticity of the error term is immediate from the first statement, since the other summands in (4.8) are analytic on $\tilde{\Omega}$. To prove the first statement, we use Lemma 4.3.1 to expand the hypergeometric functions in (4.7), obtaining

$$B(z) = f(z) + \log(1 - \phi(z))g(z), \tag{4.10}$$

for $|1 - \phi(z)| < 1$, where

$$f(z) = \frac{1}{30z^5} \left[R_1(z) \left(C_{\frac{1}{3},\frac{2}{3}} + S_{\frac{1}{3},\frac{2}{3}}(\phi(z)) \right) + R_2(z) \left(C_{\frac{2}{3},\frac{4}{3}} + S_{\frac{2}{3},\frac{4}{3}}(\phi(z)) \right) \right] + P(z),$$

and

$$g(z) = \frac{1}{30z^5}\left[R_1(z)\left(T_{\frac{1}{3},\frac{2}{3}}(\phi(z))\right) + R_2(z)\left(T_{\frac{2}{3},\frac{4}{3}}(\phi(z))\right)\right].$$

The next step in finding a singular expansion for B is to expand f and g in powers of $(1-7z)$. This simply amounts to a Taylor expansion, but for convenience we use SAGE. We find, as in our saddle-point analysis from Proposition 4.2.1, significant cancellation of lower-order terms. Specifically, we have the following Taylor expansions, convergent in a neighborhood of $1/7$:

$$f(z) = \sum_{n\geq 0}^{\infty} f_n(1-7z)^n,$$

where

$$f_0 = 7\cdot\frac{85575 - 15552\sqrt{3}}{5\pi};$$

and

$$g(z) = \sum_{n\geq 6}^{\infty} g_n(1-7z)^n,$$

where

$$g_6 = -\frac{K}{6!}, \tag{4.11}$$

with K as in (1.17). In particular, we recover the value of ρ, which was already determined in Proposition 4.3.1, from the identity

$$f_0 = f(1/7) = B(1/7) = 7/\rho.$$

Moving forward, we make the change of variable $Z = 1-7z$, and we write (4.10) as

$$B(z) = F(Z) + Z^6 G(Z)\log(1-\phi(z)), \tag{4.12}$$

where $F(Z) = f(z)$ and $G(Z) = g(z)/Z^6$ are power series convergent near $Z = 0$ with non-vanishing constant terms.

We have

$$
\begin{aligned}
B(z) &= F(Z) + Z^6 G(Z)\log(1-\phi(z)) \\
&= F(Z) + Z^6 G(Z)(\log[(1-\phi(z))/(1-7z)] + \log(1-7z)) \\
&= F(Z) + Z^6 G(Z)(\log[(2z+1)^2/(1-z)^3] + \log(1-7z)) \\
&= P(Z) + Z^7\tilde{F}(Z) + Z^6\tilde{G}(Z) + Z^6 G(Z)\log Z, \qquad (4.13)
\end{aligned}
$$

with the following definitions:

$$
\begin{aligned}
P(Z) &= \sum_{n=0}^{6} f_n Z^n\,, \\
\tilde{F}(Z) &= (F(Z)-P(Z))/Z^7 = \sum_{n\geq 7} f_n Z^{n-7}\,, \\
\tilde{G}(Z) &= G(Z)\log[(2z+1)^2/(1-z)^3]\,.
\end{aligned}
$$

Note that $\tilde{G}(0) = g_6\log(21/8) = (-K/6!)\log(21/8)$, and (4.13) is valid in a neighborhood of $z = 1/7$ in $\tilde{\Omega}$. It follows from (4.13) that

$$
B(z) = P(Z) + g_6 Z^6\log(Z) + Z^7\tilde{F}(Z) + Z^6\tilde{G}(Z) + Z^7 H_1(Z)\log Z, \qquad (4.14)
$$

where $H_1(Z) = (G(Z)-g_6)/Z$. Define the degree-six polynomial $p(Z)$ by

$$
\begin{aligned}
p(Z) = P(Z) + Z^6\tilde{G}(0) &= \left(\sum_{n=0}^{6} f_n Z^n\right) + g_6\log\left(\frac{21}{8}\right) Z^6 \qquad (4.15)\\
&= \left(\sum_{n=0}^{6} f_n Z^n\right) - \frac{K}{6!}\log\left(\frac{21}{8}\right) Z^6\,.
\end{aligned}
$$

Setting $H_2(Z) = \tilde{F}(Z) + (\tilde{G}(Z)-\tilde{G}(0))/Z$, we obtain (4.8) from (4.11) and (4.14). □

4.3.2.2. *Proof of Theorem 1.4.1(c).* Now we are in a position to verify (1.21) and (1.22). To proceed we need the following lemma.

LEMMA 4.3.2. *For $n > k \geq 0$,*

$$
[x^n][(1-x)^k\log(1-x)] = (-1)^{k+1}\frac{k!}{(n)_k}\,, \qquad (4.16)
$$

where $(n)_k = n(n-1)\cdots(n-k)$.

Proof. For $k=0$, this is just the expansion $\log(1-x) = -\sum_{n\geq 1}(x^n/n)$. For $k \in \mathbb{N}$ the result follows by induction. $\square$

It follows from (4.16) that

$$[z^n]\left(-\frac{K}{6!}Z^6 \log Z\right) = \frac{K\cdot 7^n}{(n)_6}.$$

From this fact, along with (4.8) and Theorem 1.4.4, we find the following improvement to Proposition 4.2.1:

$$b_n = K\cdot 7^n\left(\frac{1}{n^7} + \mathcal{O}\left(\frac{\log n}{n^8}\right)\right), \quad \text{as } n\to\infty. \tag{4.17}$$

We can take this analysis a step further to expand b_n in an asymptotic series. Indeed, recalling the expansion $g(z) = \sum_{n\geq 6} g_n Z^n$ from above, a careful look at the derivation of (4.8) from (4.13) in the proof of Proposition 4.3.2 shows that B can be written as

$$B(z) = \tilde{p}(Z) + g_6 Z^6 \log Z + g_7 Z^7 \log Z + Z^8 \tilde{H}_2(Z) + Z^8 \tilde{H}_1(Z)\log Z\,, \tag{4.18}$$

for

$$\begin{aligned}\tilde{p}(Z) &= p(Z) + Z^7 H_2(0)\,,\\ \tilde{H}_1(Z) &= (H_1(Z) - g_7)/Z\,,\\ \tilde{H}_2(Z) &= (H_2(Z) - H_2(0))/Z\,.\end{aligned}$$

We have simply extracted the higher order term $g_7 Z^7 \log Z$ from $g(z)\log(Z)$ to get a more accurate estimate of B near $Z=0$. In the same way that we derived (4.17), we find from (4.16) and (4.18) that

$$b_n = 7^n\left(\frac{K}{n^7} + \frac{\tilde{K}}{n^8} + \mathcal{O}\left(\frac{\log n}{n^9}\right)\right),$$

where $\tilde{K} = 7! g_7$. This shows that the $\mathcal{O}(n^{-8}\log n)$ term in (4.17) is actually $\mathcal{O}(n^{-8})$, so we obtain the asymptotic expression (1.21).

One sees moreover that the process can be continued indefinitely, which yields the asymptotic series

$$\frac{b_n}{7^n} \sim \sum_{i=7}^{\infty} \frac{K_i}{n^i},$$

where $K_7 = K$, $K_8 = \tilde{K}$, and in general $K_n = (-1)^n (n-1)! g_{n-1}$. Since

$$\Gamma\left(\frac{2}{3}\right)\Gamma\left(\frac{4}{3}\right) = \frac{1}{3}\Gamma\left(\frac{1}{3}\right)\Gamma\left(\frac{2}{3}\right) = \frac{2\pi}{3\sqrt{3}},$$

as in the proof of Proposition 4.3.1, inspecting the definition of $g(z)$ from (4.10) and the definition of $T_{a,b}$ from (4.9) shows that each K_i is a rational multiple of $\sqrt{3}/\pi$, so that with $\kappa_i = K_i \pi/\sqrt{3}$ for $i \geq 7$, we have verified (1.22).

4.3.2.3. *Three auxiliary constants.* It will be useful in the sequel to define

$$\lambda := (1/7)B'(1/7) = -f_1\,. \tag{4.19}$$

Of course, one may object that B is not analytic at $1/7$, but (4.8) shows that $B'(1/7)$ still exists as the limit of $B'(z)$, as $z \to 1/7$ in $\tilde{\Omega}$, and has the value $-7p'(0) = -7P'(0) = -7f_1$. Using simplifications like those used to evaluate ρ in Proposition 4.3.1, the value of λ is seen to be

$$\lambda = \frac{852768\sqrt{3} - 470155\pi}{10\pi} \approx 0.0639\,.$$

We also record for later that

$$y'\left(\frac{1}{7}\right) = \frac{1}{7}B'\left(\frac{1}{7}\right) + B\left(\frac{1}{7}\right) = \lambda + \frac{7}{\rho} \approx 1.0901\,, \tag{4.20}$$

and that

$$A'\left(\frac{1}{\rho}\right) = 7 - \frac{49}{\rho\lambda + 7} \approx 0.4106\,, \tag{4.21}$$

which can be deduced by differentiating (4.1) and evaluating at $1/7$, obtaining

$$y'(1/7) = A'(y(1/7))y'(1/7) + A(y(1/7)) = A'(1/\rho)y'(1/7) + 7/\rho\,,$$

and then substituting (4.20). The $\approx$ symbol indicates an error of less than 10^{-5}, which could be checked from rational approximations of π and $\sqrt{3}$.

4.3.2.4. *Alternative proof of Conjecture 1.4.1.* From the preceding analysis we obtain the following proof by contradiction. Assume $y(r) = rB(r) < R$, where $r = 1/7$ and R is the radius of convergence of A. Then by Theorem 4.1.1 and (4.4), we see that $\psi'(y(r)) = 0$, and this implies that $y'(r) = \infty$, by the inverse function theorem. But $y'(r) < \infty$ from (4.20), so $rB(r) = R$.

As a technical point, since B is not analytic at $1/7$, the values of B' and y' from (4.4) are actually limits of $y(z)$ as $z \to 1/7$ in $\tilde{\Omega}$, so the inverse function theorem does not strictly apply. But one can just apply the real inverse function theorem to $\psi'(y(z))$ as $z \to 1/7$ along $(0, 1/7)$.

4.3.3. Analytic continuation of ψ. We introduce the domain

$$\Lambda := \{z : |z| < 1/\rho\}.$$

Recall from Lemma 4.1.2 that the function ψ, defined by $\psi(z) = z/A(z)$, is analytic on $y(\Omega)$. Also recall from (1.19) that the radius of convergence of A is $1/\rho$, so that by Pringsheim's Theorem, $1/\rho$ is a singularity of A and so also of ψ.

Observe that $y(\Omega) \subset \Lambda$ by the triangle inequality, since $y_n \geq 0$ for all $n \geq 0$, while Lemma 4.1.2 implies that $(y \circ \psi)|_{y(\Omega)} = \mathrm{Id}\,|_{y(\Omega)}$. We would like to continue ψ analytically to Λ, and then to a Delta-domain around Λ, and we would like to maintain the inverse relationship between y and ψ. In other words, we seek to establish the following proposition.

Proposition 4.3.3. *The function ψ is analytically continuable to a Delta-domain $\Delta_{1/\rho}$ around Λ. Furthermore,*

$$(y \circ \psi)|_{\Delta_{1/\rho}} = \mathrm{Id}\,|_{\Delta_{1/\rho}}.$$

Before the proof we establish two lemmas.

Lemma 4.3.3. *ψ is analytic on Λ with non-vanishing derivative, and ψ and ψ' extend continuously to $\partial\Lambda$.*

Proof. We begin with a numerical evaluation. (4.1) implies $A(y(1/7)) = 7/\rho \approx 1.0262$, where ρ was evaluated in Proposition 4.3.1.

It follows that $\sum_{n\geq 1} a_n y(1/7)^n < 1$, and hence $\sum_{n\geq 1} a_n z^n < 1$ for $|z| \leq y(1/7)$, since $a_n \geq 0$ for all n. Since $A(0) = 1$, this implies that A doesn't vanish on $\overline{\Lambda}$. Therefore, ψ is analytic not only on $y(\Omega)$, but also on Λ, and extends continuously to $\partial\Lambda$ by the Weierstrass M-test applied to $A(x)$.

To verify that ψ' does not vanish on Λ, recall (4.4), namely that

$$\psi'(z) = \frac{A(z) - zA'(z)}{A(z)} = \frac{1}{A(z)} \left(1 + \sum_{n \geq 1} a_n (1-n) z^n \right).$$

The quantity $A(z) - zA'(z)$ doesn't vanish on $(0, y(1/7))$, e.g. by Theorem 4.1.3 and the fact that $y_n \sim K7^n/n^7$. Since $a_n \geq 0$, this implies that $\sum_{n \geq 1} a_n(n-1)z^n < 1$ for all $z \in (0, y(1/7))$, so $A(|z|) - |z|A'(|z|) > 0$ for $z \in \Lambda$ and ψ' doesn't vanish on Λ. (4.21) shows that $A'(y(1/7))$ is finite, so the Weierstrass M-test implies that $A'(z)$ and $\psi'(z)$ extend continuously to $\partial\Lambda$. $\square$

Although the lemma extends ψ beyond $y(\Omega)$ to all of Λ, it does not automatically imply that $\psi(\Lambda) \subset \tilde{\Omega}$, or, in other words, that ψ avoids the branch cuts $(\infty, -1/2]$ and $[1/7, \infty)$. We resolve this doubt in the following lemma.

LEMMA 4.3.4. *$\psi(\Lambda) \subset \tilde{\Omega}$, y is analytic on $\psi(\Lambda)$, and $(y \circ \psi)|_\Lambda = \mathrm{Id}\,|_\Lambda$.*

PROOF. The proof is based on two complementary claims about ψ, which is continuous on $\overline{\Lambda}$ by Lemma 4.3.3.

Claim 1: If $z \in \overline{\Lambda} \setminus \mathbb{R}$, then $\psi(z) \notin \mathbb{R}$.

To see why this is true, suppose toward showing the contrapositive that $\psi(z) \in \mathbb{R}$. Then $A(z) = \beta z$ for some $\beta \in \mathbb{R}$. Observe that $\rho > 6.8$ by Proposition 4.3.1, so that $y(1/7) = 1/\rho < 0.15$, and this implies that $6/\rho < 2 - 7/\rho$. From $\beta z = 1 + (A(z) - 1)$, we see that

$$\begin{aligned} |\beta z| &\geq 1 - \sup_{w \in \Lambda} |A(w) - 1| = 1 - (A(1/\rho) - 1) \\ &= 2 - 7/\rho > 6/\rho \\ &> 6|z|. \end{aligned}$$

It follows that $6 < |\beta|$.

On the other hand, since $A(z) = \beta z$, we see that $A(\overline{z}) = \overline{A(z)} = \beta\overline{z}$. It follows that

$$\beta(z - \overline{z}) = A(z) - A(\overline{z}) = \int_{\overline{z}}^{z} A'(w)\, dw,$$

where the integration path is the line segment from $\overline{z}$ to z, as Λ is convex, and therefore

$$|\beta| \cdot |z - \overline{z}| \leq |z - \overline{z}| \cdot \sup_{w \in \Lambda} |A'(w)|.$$

Since A has non-negative Taylor coefficients, A' is bounded by $A'(1/\rho) < 1$, from (4.21). If $z \neq \overline{z}$, this would imply that $|\beta| \leq 1$, which is impossible since we already showed that $|\beta| > 6$. It follows that $z = \overline{z}$, verifying the claim.

Claim 2: ψ maps $\overline{\Lambda} \cap \mathbb{R} = [-1/\rho, 1/\rho]$ bijectively onto $[\psi(-1/\rho), 1/7] \subset (-1/2, 1/7]$.

To see why this is true, note that ψ maps the interval $[y(-1/7), 1/\rho]$ bijectively to $[-1/7, 1/7]$ by Lemma 4.1.2, so it remains only to consider $[-1/\rho, y(-1/7))$. Since $\psi'(0) = 1$, and ψ' is non-vanishing on Λ by Lemma 4.3.3, we see that ψ is increasing on $[-1/\rho, y(-1/7))$ and maps the latter interval onto $[\psi(-1/\rho), -1/7)$. In the proof of Lemma 4.3.3 we approximated $A(1/\rho)$, and here the estimate $A(1/\rho) < 3/2$ is sufficient, since then we have $A(-1/\rho)) > 1/2$, and therefore

$$|\psi(-1/\rho)| = \frac{1/\rho}{A(-1\rho)} < 2/\rho < 1/2,$$

which verifies the claim.

Taken together, the two claims show that $\psi(\Lambda) \subset \tilde{\Omega}$, as desired. It follows that y is analytic on $\psi(\Lambda)$, and $(y \circ \psi)|_\Lambda = \mathrm{Id}\,|_\Lambda$ by the principle of permanence, since $(y \circ \psi)|_{y(\Omega)} = \mathrm{Id}\,|_{y(\Omega)}$ and $y(\Omega) \subset \Lambda$.

□

Proof of Proposition 4.3.3. Now we are ready to extend ψ analytically to a Delta-domain $\Delta_{1/\rho}$. It will he helpful to set $\alpha := y'(1/7)$ for the rest of the proof. Recall from (4.20) that $\alpha > 0$ and from (4.8) that y' is continuous at $1/7$. Choose E to be an open ball centered at $1/7$, such that $|y'(w) - \alpha| < \alpha/9$ for $w \in \tilde{\Omega} \cap E$. For $z_1, z_2 \in \tilde{\Omega} \cap E$, let γ be any path from z_1 to z_2 in $\tilde{\Omega} \cap E$, and denote by L the length of γ. Since

$$y(z_1) - y(z_2) = \int_\gamma y'(w)\,dw = \int_\gamma \alpha\,dw + \int_\gamma [y'(w) - \alpha]\,dw\,,$$

it follows that

$$\begin{aligned}|y(z_1) - y(z_2)| &\geq \left|\int_\gamma \alpha\,dw\right| - \left|\int_\gamma [y'(w) - \alpha]\,dw\right| \geq \alpha L - L \cdot \sup_{w \in \tilde{\Omega} \cap N} \left|y'(w) - \alpha\right| \\ &\geq \alpha L - \frac{\alpha}{9} L \geq \frac{8\alpha}{9} |z_1 - z_2|\,.\end{aligned}$$

Since $\alpha \neq 0$, we see that $|y(z_1) - y(z_2)| = 0$ implies $z_1 = z_2$, so y admits an inverse function on $\tilde{\Omega} \cap E$, which we call y^{-1}, and which is analytic on $y(\tilde{\Omega} \cap E)$ as the inverse of an analytic map [**Hil59**, Ch. 9.4]. Taking limits as $z_2 \to 1/\rho$ in the integral estimate above, we see that

$$|y(z) - 1/\rho| \geq \frac{8\alpha}{9}|z - 1/7| \tag{4.22}$$

for $z \in \tilde{\Omega} \cap E$. Reversing the inequality in the integral estimate yields

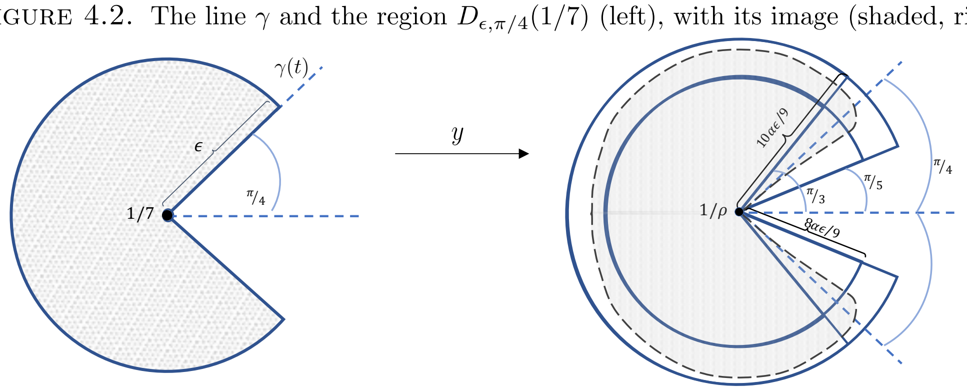
$$|y(z) - 1/\rho| \leq \frac{10\alpha}{9}|z - 1/7|\,. \tag{4.23}$$

Next, for $z \in \mathbb{C}$, $\epsilon > 0$, and $\delta \in (0, \pi/2)$, define the open set

$$D_{\epsilon,\delta}(z) := \{w : |w - z| < \epsilon, |\mathrm{Arg}(w - z)| > \delta\}.$$

We claim that ψ can be continued analytically to $D_{\epsilon,\delta}(1/\rho) \subset \tilde{\Omega} \cap E$, for some $\epsilon > 0$ and some $\delta \in (0, \pi/2)$. The basic idea is that $\alpha > 0$ has the geometric implication that near $1/7$ the map $z \mapsto y(z)$ acts approximately as a dilation. That is, for some small $\epsilon > 0$, and $\delta = \pi/4$, say, y maps the region $D_{\epsilon,\delta}(1/7)$ onto an open set that is a slight perturbation of $D_{\alpha\epsilon,\pi/4}(1/\rho)$ (see Figure 4.2), and ψ is extended to $D_{\alpha\epsilon,\pi/4}(1/\rho)$ by the local inverse of y.

FIGURE 4.2. The line γ and the region $D_{\epsilon,\pi/4}(1/7)$ (left), with its image (shaded, right).



In full detail, if γ is a straight line emanating from $1/7$, of the form $\gamma(t) = 1/7 + te^{i\pi/4}$ for $t \geq 0$, then since $\alpha > 0$, there is some $T > 0$ such that $\pi/5 < \mathrm{Arg}(y(\gamma(t)) - 1/\rho) < \pi/3$ for every $t \in (0, T)$. The Schwarz Reflection Principle implies that $y(\overline{z}) = \overline{y(z)}$, so for $t \in (0, T)$ we also have $-\pi/5 > \mathrm{Arg}(y(\gamma_2(t)) - y(1/7)) > -\pi/3$, where $\gamma_2(t) = 1/7 + te^{-i\pi/4}$. Now choose some $\epsilon > 0$ that is smaller than both T and the radius of the ball E from above. If $|z - 1/7| = \epsilon$ for $z \in \tilde{\Omega}$, then we have from estimates (4.22) and (4.23) that

$$\frac{8\alpha\epsilon}{9} \leq |y(z) - 1/\rho| \leq \frac{10\alpha\epsilon}{9}\,.$$

Thus, we have described the images of the two line segments and the circular arc that make up the boundary of $D_{\epsilon,\pi/4}$, and our description implies that the image of $D_{\epsilon,\pi/4}(1/7)$ contains the open set $D_{8\alpha\epsilon/9,\pi/3}(1/\rho)$, as shown in Figure 4.2. We also saw above that y^{-1} is analytic on $y(\tilde{\Omega} \cap E)$ and hence on $D_{8\alpha\epsilon/9,\pi/3}(1/\rho)$, which intersects Λ in a nonempty open set. Thus, if we redefine ϵ to denote the value $8\alpha\epsilon/9$ from above, and also set $\delta = \pi/3$, then y^{-1} extends ψ to $D_{\epsilon,\delta}(1/\rho)$, as was to be shown. By construction we have the inverse relationship $(y \circ \psi)|_{D_{\epsilon,\delta}(1/\rho)} = \mathrm{Id}\,|_{D_{\epsilon,\delta}(1/\rho)}$.

To finish extending ψ to $\Delta_{1/\rho}$, it suffices by compactness of the set $\partial\Lambda \setminus D_{\epsilon,\delta}(1/\rho)$ to obtain analytic continuations of ψ around all points in an arbitrary finite subcollection of $\partial\Lambda \setminus \{1/\rho\}$.

Let $\tilde{w} \in \partial\Lambda \setminus \{1/\rho\}$. The two supporting claims in the proof of Lemma 4.3.4 imply that $\psi(w) \in \tilde{\Omega}$. We claim that $y'(\psi(\tilde{w})) \neq 0$. To see why this is true, let γ be the straight line path from 0 to $\tilde{w}$. If $0 = y'(\psi(\tilde{w}))$, then recalling from Lemma 4.3.4 that $y \circ \psi = \mathrm{Id}\,|_\Lambda$ we see that $y(\psi(w)) = w$ for $w \in \gamma$. Therefore,

$$0 = \lim_{w \to \tilde{w}, w \in \gamma} |y'(\psi(w))| = \lim_{w \to \tilde{w}, w \in \gamma} 1/|\psi'(w)|,$$

which implies that $|\psi'(w)| \to \infty$ as $w \to \tilde{w}$ along γ. This contradicts the fact from Lemma 4.3.3 that ψ' extends continuously to $\partial\Lambda$ and so is bounded there. So $y'(\psi(\tilde{w})) \neq 0$. By the inverse function theorem, y is locally invertible at $\psi(\tilde{w})$, and the local inverse extends ψ analytically to a neighborhood of $\tilde{w}$ that maps into $\tilde{\Omega}$.

We have extended ψ to a Delta-domain $\Delta_{1/\rho}$ by patching together *local* inverses of y. To see that y is a *global* inverse of ψ, one need only observe that $\psi(\Delta_{1/\rho}) \subset \tilde{\Omega}$, by construction. It follows that y is analytic on $\psi(\Delta_{1/\rho})$, and $(y \circ \psi)|_{\Delta_{1/\rho}} = \mathrm{Id}\,|_{\Delta_{1/\rho}}$ by the principle of permanence. □

4.3.4. Asymptotic singular expansion of ψ near $y(1/7)$. Let $\Delta_{1/\rho}$ be the Delta-domain from Proposition 4.3.3. We apply a "bootstrapping" procedure to (4.8) that locally inverts y near 1/7, up to an asymptotically negligible error term, resulting in an asymptotic singular expansion for $\psi = y^{-1}$ near the singularity $1/\rho$ (the general idea of bootstrapping and some examples are discussed in [**DB58**, Ch. 2]). Precisely, we show the following, with λ as in (4.19).

Proposition 4.3.4. *Set $V = 1 - \rho z$. The function ψ admits the following singular expansion: as $z \to 1/\rho$ in $\Delta_{1/\rho}$,*

$$\psi(z) = \gamma(V) + CV^6 \log V + \mathcal{O}(V^7 \log V), \tag{4.24}$$

where

$$C = \frac{7^5 K\rho}{6!(7+\rho\lambda)^7},$$

and γ is a degree-six polynomial with $\gamma(0) = 1/7$. Furthermore, the error term $\psi(z) - \gamma(V) - CV^6 \log V$ is analytic in $\Delta_{1/\rho}$.

Before the proof we illustrate the bootstrapping technique with a small example, which could also be skipped.

Example 4.3.1. Consider the equation $z = w + w^2 + w^2 \log w$. Then $w \sim z$, as $w, z \to 0$, and $\log z = \log w + \log(1 + w + w \log w) = \log w + \mathcal{O}(w \log w)$. It follows that $\log w = \log z + \mathcal{O}(z \log z)$. Since $w = z - w^2 + w^2 \log w$, we therefore have $w^2 = z^2 + \mathcal{O}(z^3 \log z)$. Plugging back into the original equation, this yields

$$w = z - z^2 - z^2 \log z + \mathcal{O}(z^3 \log z).$$

The proof of the proposition is similar, but more involved.

Proof of Proposition 4.3.4. With $Z = 1 - 7z$, (4.8) implies that

$$y(z) = \frac{1-Z}{7}\left(p(Z) - \frac{K}{6!}Z^6 \log Z + \mathcal{O}(Z^7 \log Z)\right),$$

as $z \to 1/7 \in \tilde{\Omega}$. By the identity $(y \circ \psi)|_{\Delta_{1/\rho}} = \mathrm{Id}\,|_{\Delta_{1/\rho}}$, if we evaluate both sides of the equation at $\psi(z)$, for z in a small neighborhood of $1/\rho$ in $\Delta_{1/\rho}$, and if we apply the change of variables $Y = 1 - 7\psi(z)$, then we obtain

$$\frac{1-Z}{7} = z = y(\psi(z)) = \frac{1-Y}{7}\left(p(Y) - \frac{K}{6!}Y^6 \log(Y) + \mathcal{O}(Y^7 \log Y)\right),$$

which implies

$$Z - 1 = (Y-1)\left(p(Y) - \frac{K}{6!}Y^6 \log Y + \mathcal{O}(Y^7 \log Y)\right), \tag{4.25}$$

as $z \to 1/\rho$ in $\Delta_{1/\rho}$. In (4.15) we see that $p(Y) = (-K/6!)\log(21/8)Y^6 + \sum_{n=0}^{6} f_n Y^n$. Thus, upon setting

$$W = \frac{Z + f_0 - 1}{f_0 - f_1},$$

we find from (4.25) that as $z \to 1/\rho$ in $\Delta_{1/\rho}$,

$$Y = W - (Q(Y) + cY^6 \log Y + \mathcal{O}(Y^7 \log Y)), \tag{4.26}$$

where

$$Q(Y) = \frac{f_1 - f_2}{f_0 - f_1}Y^2 + \frac{f_2 - f_3}{f_0 - f_1}Y^3 + \frac{f_3 - f_4}{f_0 - f_1}Y^4 + \frac{f_4 - f_5}{f_0 - f_1}Y^5 + \frac{f_5 - f_6 + \frac{K}{6!}\log\left(\frac{21}{8}\right)}{f_0 - f_1}Y^6,$$

and

$$c = \frac{K}{6!(f_0 - f_1)} = \frac{K}{6!(7/\rho + \lambda)}\,.$$

For simpler notation, define the list of constants $(a_i)_{i=2}^{6} \subset \mathbb{R}$ so that $Q(Y) = \sum_{i=2}^{6} a_i Y^i$.

$W(z)$ and $Y(z)$ tend to 0 as $z \to 1/\rho$ in $\Delta_{1/\rho}$. It follows then from (4.26) that $W \sim Y$ as $z \to 1/\rho$. Therefore, $Y = \mathcal{O}(W)$ and $\log(Y) \sim \log(W)$ (as $z \to 1/\rho$ in $\Delta_{1/\rho}$, which is assumed for the rest of the proof). These estimates for Y imply that

$$Q(Y) = a_2 W^2 + \mathcal{O}(W^3)\,,$$

which, upon substitution into (4.26), yields

$$Y = W - a_2 W^2 + \mathcal{O}(W^3).$$

We substitute this new estimate for Y into $Q(Y)$, which yields

$$Q(Y) = a_2 W^2 + (a_3 - 2a_2^2)W^3 + \mathcal{O}(W^4),$$

and hence, from (4.26),

$$Y = W - a_2 W^2 - (a_3 - 2a_2^2)W^3 + \mathcal{O}(W^4).$$

After another iteration, we obtain from (4.26) that

$$\begin{aligned} Y &= W - Q(Y) + \mathcal{O}(W^5) \\ &= W - a_2W^2 - (a_3 - 2a_2^2)W^3 - (5a_2^3 - 5a_2a_3 + a_4W^4) + \mathcal{O}(W^5). \end{aligned}$$

After a final iteration, we obtain from (4.26) that

$$Y = W - a_2W^2 - \cdots - a_6'W^6 + \mathcal{O}(W^7) + cY^6 \log Y + \mathcal{O}(Y^7 \log Y),$$

where a_6' is an unimportant constant. Since $Y = W + \mathcal{O}(W^2)$, we have that the $\mathcal{O}(Y^7 \log Y)$ error term is $\mathcal{O}(W^7 \log W)$, and that $Y^6 \log Y = W^6 \log W + \mathcal{O}(W^7 \log W)$. We can therefore express Y in terms of W as follows:

$$Y = W - a_2W^2 - \cdots - a_6'W^6 + cW^6 \log W + \mathcal{O}(W^7 \log W)\,.$$

We substitute $\psi(z) = (1 - Y)/7$ in the latter expression, obtaining

$$\psi(z) = \frac{1}{7} + \tilde{P}(W) + \frac{c}{7}W^6 \log(W) + \mathcal{O}(W^7 \log W), \tag{4.27}$$

with $\tilde{P}(0) = 0$.

To finish the proof, it just remains to write W in terms of V:

$$W = \frac{Z + f_0 - 1}{f_0 - f_1} = \frac{Z + 7/\rho - 1}{7/\rho + \lambda} = \frac{7/\rho - 7z}{7/\rho + \lambda} = \frac{7}{7 + \rho\lambda}(1 - \rho z) = \frac{7}{7 + \rho\lambda}V\,.$$

Substituting the last expression into (4.27) leads immediately to (4.24), with

$$\gamma(V) = \frac{1}{7} + \tilde{P}\left(\frac{7}{7 + \rho\lambda}V\right),$$

and

$$C = \frac{c}{7}\left(\frac{7}{7 + \rho\lambda}\right)^6 = \frac{7^5 K\rho}{6!(7 + \rho\lambda)^7}\,.$$

The error term in (4.27) is analytic in $\Delta_{1/\rho}$ since all the other terms are. $\square$

4.3.5. Asymptotic singular expansion of A near $y(1/7)$. Since ψ is injective on $\Delta_{1/\rho}$ by Proposition 4.3.3, and $\psi(0) = 0$, we see that $A(z) = z/\psi(z)$ extends to be analytic on $\Delta_{1/\rho}$. We seek its singular expansion near $1/\rho = y(1/7)$. Let C be the constant from Proposition 4.3.4.

Proposition 4.3.5. *Set $V = 1 - \rho z$. The function A admits the following singular expansion: as $z \to 1/\rho$ in $\Delta_{1/\rho}$,*

$$A(z) = \eta(V) - \frac{49C}{\rho} V^6 \log V + \mathcal{O}(V^7 \log V), \tag{4.28}$$

where η is a degree-seven polynomial. The error term $A(z) + (49C/\rho)V^6 \log V - \eta(V)$ is analytic in $\Delta_{1/\rho}$.

Proof. Referring to Proposition 4.3.4, let $E(V)$ denote the error term in (4.24), namely,

$$E(V) = \psi(z) - \gamma(V) - CV^6 \log V.$$

$E(V)$ is visibly analytic on $\Delta_{1/\rho}$. Let $(b_i)_{i=0}^6 \subset \mathbb{R}$ be such that $\gamma(V) = \sum_{i=0}^6 b_i V^6$ (e.g. $b_0 = 1/7$). Define the polynomial

$$\begin{aligned} T(V) = &-49\left(49b_2^3 - 7b_3^2 - 14b_2b_4 + b_6\right)V^6 + 49\left(14b_2b_3 - b_5\right)V^5 \\ &+ 49\left(7b_2^2 - b_4\right)V^4 - 49b_3V^3 - 49b_2V^2 + 7\,. \end{aligned} \tag{4.29}$$

Also define $S(V) = T(V) - 49CV^6 \log V$, which is analytic on $\Delta_{1/\rho}$.

A routine computation shows that

$$\begin{aligned} \psi(z)S(V) &= \left[\left(\frac{1}{7} + \sum_{i=1}^{6} b_i V^i\right) + CV^6 \log V + E(V)\right]\left[T(V) - 49CE(V)V^6 \log V\right] \\ &= 1 + E(V)T(V) - 49CE(V)V^6 \log(V) + \left[\sum_{i=7}^{12} V^i \cdot d_i(\log V)\right], \end{aligned}$$

where $d_i(x)$ is a linear polynomial, for $7 \le i \le 11$, and $d_{12}(x)$ is a quadratic polynomial. It follows that

$$\tilde{E}(V) := \psi(z)S(V) - 1$$

is analytic on $\Delta_{1/\rho}$ and $\mathcal{O}(V^7 \log V)$ as $z \to 1/\rho$ in $\Delta_{1/\rho}$. We write this as

$$\frac{1}{\psi(z)} = S(V) - \frac{\tilde{E}(V)}{\psi(z)},$$

or, since $z = (1-V)/\rho$,

$$A(z) = \frac{z}{\psi(z)} = \frac{(1-V)}{\rho} S(V) - A(z)\tilde{E}(V).$$

Comparing the latter equation with (4.29), we see that

$$A(z) = -\frac{49C}{\rho} V^6 \log(V) + \eta(V) + \tilde{\tilde{E}}(V)\,,$$

where

$$\eta(V) = \frac{1-V}{\rho}(S(V) + 49CV^6 \log V)$$

is a degree-seven polynomial, and the error term

$$\tilde{\tilde{E}}(V) := \frac{49C}{\rho} V^7 \log(V) - A(z)E\tilde{(V)}$$

is analytic in $\Delta_{1/\rho}$ and $\mathcal{O}(V^7 \log V)$ as $z \to 1/\rho$. $\square$

4.3.6. Asymptotic formula for (a_n). By (4.16), (4.28), and Theorem 1.4.4, we have

$$a_n = \frac{49 \cdot C \cdot 6!}{\rho} \cdot 7^n \left(\frac{1}{n^7} + \mathcal{O}\left(\frac{\log n}{n^8} \right) \right),$$

as $n \to \infty$. Since $49 \cdot C \cdot 6!$ is precisely the constant M from (1.18), this verifies (1.23) and completes the proof of Theorem 1.4.1.

4.4. The case of the Lie algebra B_2

In this final section of the chapter we consider the analogous sharpness question from Kuperberg's conjecture for the Lie algebra B_2, which is a rank-2 Lie algebra of dimension 10. We will follow the discussion on OEIS [**SI20**] for the sequences indexed by A005700 and A194091. Although our presentation will be somewhat informal, we hope to indicate how some of the preceding ideas can be used in other situations.

We define the sequence $(d_n)_{n=0}^{\infty}$ analogously to $(b_n)_{n=0}^{\infty}$, except that we modify for the fact that $\dim \mathrm{Inv}_{B_2}(V(\lambda_1)^{\otimes n}) = 0$ when n is odd, where λ_1 is the fundamental weight for B_2 with a 4-dimensional representation. Thus $d_0 := 1$, and for $n \geq 1$ we define (OEIS: A005700)

$$d_n = \dim \mathrm{Inv}_{B_2}(V(\lambda_1)^{\otimes 2n})\,.$$

The sequence begins

$$(d_n)_{n0}^{\infty} = 1, 1, 3, 14, 84, 594, 4719, 40898, 379236, 3711916, \ldots$$

Similar to the numbers b_n in the case of G_2, the numbers d_n can be interpreted as counting the lattice paths of length $2n$ that start and end at the origin and are confined to the first octant of $\{(x, y) : 0 \leq x \leq y\} \subset \mathbb{Z}^2$, the dominant Weyl chamber for B_2. An explicit formula is given for $n \geq 0$ by

$$d_n = \frac{6(2n)!(2n+2)!}{n!(n+1)!(n+2)!(n+3)!},$$

which is the nth Taylor coefficient of the hypergeometric generating function

$$D(x) = \sum_{n=0}^{\infty} d_n x^n = {}_3F_2\left(1, \frac{1}{2}, \frac{3}{2}; 3, 4; 16x\right).$$

As $n \to \infty$, Stirling's formula leads to the approximation

$$d_n = \Theta\left(\frac{16^n}{n^5}\right) = \Theta\left(\frac{\dim(V(\lambda_1))^{2n}}{n^{(\dim B_2)/2}}\right).$$

Next, we describe the analogue of the sequence (a_n) from the G_2 case. Instead of triangulations of a regular n-gon, we set $c_0 = 1$ and for $n > 0$ define c_n to be the number of *quadrangulations* of a regular $2n$-gon (every internal face is a quadrilateral), such that each internal vertex has degree at least 4. The sequence (OEIS: A194091) begins

$$(c_n)_{n\geq 0} = 1, 1, 1, 3, 14, 82, 554, 4132, 33154, 281459, \ldots$$

Setting $C(x) = \sum_{n=0}^{\infty} c_n x^n$ and $D(x) = \sum_{n=0}^{\infty} d_n x^n$, we have the functional equation

$$D(x) = C(xD(x)^2). \tag{4.30}$$

This formula has been conjectured on the OEIS page cited above. We sketch now how to derive it.

The functional equation (1.15) – $B(x) = A(xB(x))$ – arises from expressing $\mathrm{Inv}_{G_2}(V(\lambda_1)^{\otimes n})$ as isomorphic to the vector space generated by a basis consisting of *basis webs*, i.e. trivalent non-crossing planar graphs embedded in a disk with n points [**Kup96**, Thm. 6.9] (see also [**Wes07**]). Consider the restriction to the *connected* basis webs of this bijection from all basis webs to a basis of $\mathrm{Inv}_{G_2}(V(\lambda_1)^{\otimes n})$. These connected basis webs correspond to the triangulations counted by (a_n), as explained after Theorem 8.1 in [**Kup96**] (essentially by the definition of "non-elliptic" – in the terminology of the paper – and the fact that trivalent vertices can be used to generate all basis webs for this representation, as well as the duality between triangulations and connected basis webs). Then (1.15) follows from organizing the connected components of a basis web into a rooted planar tree in a particular way.

In the case of B_2, the construction is isomorphic, except that the basis webs are generated by a tetravalent vertex (as opposed to trivalent). This and the non-elliptic condition translate – upon passing to dual graphs – respectively to the properties of having each face in the cover of an n-gon be a square (not a triangle) and having each internal vertex possess no fewer than 4 (not 6) edges. What we obtain then is that

$$\tilde{D}(x) = \tilde{C}(x\tilde{D}(x))\,, \tag{4.31}$$

where $\tilde{C}(x) = \sum_{n\geq 0} \tilde{c}_n x^n$ and $\tilde{D}(x) = \sum_{n\geq 0} \tilde{d}_n x^n$ with $\tilde{c}_n$ the number of quadrangulations of an n-gon and $\tilde{d}_n = \dim \mathrm{Inv}_{B_2}(V(\lambda_1)^n)$. Since $\tilde{c}_n = \tilde{d}_n = 0$ when n is odd, we can write $C(x^2) = \tilde{C}(x)$ and $D(x^2) = \tilde{D}(x)$ to obtain (4.30).

Theorems 1.4.2 and 4.1.2 do not directly apply to (4.31), since the gcd condition is not met for the generating function $\tilde{C}(x)$, which is even. However, in the paragraph after Theorem 4.1.2 it is stated that the gcd condition is a mild technically. Indeed, as the reader would see in pursuing the references indicated there, our sharpness conclusion still follows in (4.31) by considering subsequences, i.e. from the fact that the sequence $(\tilde{d}_n)_{n\geq 0}$ is supported on the even positive integers and that $\tilde{d}_{2n}/16^n \neq \Theta(n^{-3/2})$ as $n \to \infty$. Or, an alternative argument is obtained by applying the reasoning in Remark 4.1.3 to the subsequence $(\tilde{d}_{2n})_{n\geq 0}$. In any case, one finds that the radius of convergence of $\tilde{C}(x)$ is precisely $\tilde{D}(1/4)/4$, which implies that $C(x)$ has radius of convergence $D(1/16)^2/16$. In other words, we have the following result:

Theorem 4.4.1.

$$\limsup_{n\to\infty} \sqrt[n]{c_n} = \frac{16}{D(1/16)^2} = \frac{16}{{}_3F_2\left(1, \frac{1}{2}, \frac{3}{2}; 3, 4; 1\right)^2} = \frac{225\pi^2}{4(165\pi - 512)^2}\,,$$

with an approximate value of 13.7128.

Applying Fekete's lemma as we did for (a_n) we can easily pass to the limit. Also, since $D(x)$ is given explicitly here, one could potentially use appropriate expansions of ${}_3F_2$ to give an alternative proof of asymptotic sharpness by an inverse function theorem argument, like we did in Section 4.3.2.4. With more motivation one might even deduce a true asymptotic formula by a bootstrapping procedure, as we did for (a_n).

CHAPTER 5

Expectation of the sum of binary digits in the iterated Syracuse map

To prove Theorems 1.5.2 and 1.5.3, we will eventually consider N_n, $\mathcal{S}(N_n)$, and $\mathcal{S}^2(N_n)$ to be random vectors of binary digits, and show how these digits arise from a random walk on a finite-state machine. Before doing that, we will review some useful deterministic algorithms for doing binary arithmetic, as these will be the basis for the random models. First we introduce some notation.

DEFINITION 5.0.1. Let $n \in \mathbb{Z}^+$. Let $N_n \in \mathbb{N}_{\text{odd}} \cap [1, 2^n - 1]$ and let $N_n = \sum_{i=0}^{\infty} t_i 2^i$ be its binary expansion, i.e. $t_0 = 1$, $t_i \in \{0, 1\}$ for $1 < i < n$, and $t_i = 0$ for $i \geq n$. We associate to N_n the number τ_n defined by

$$\tau_n = \omega(3N_n + 1)\,.$$

In other words, if n is even and $(t_0, t_1, \ldots, t_{n-1}) = (1, 0, 1, 0, \ldots, 0, 1, 0)$, then $\tau_n = n$; if n is odd and $(t_0, t_1, \ldots, t_{n-1}) = (1, 0, 1, 0, \ldots, 1, 0, 1)$, then $\tau_n = n + 1$; and if the first n binary digits of N_n do not alternate, then τ_n is the index of the first repeated digit in $(t_0, t_1, \ldots, t_{n-1})$.

We also associate to N_n the following numbers:

$$\begin{aligned}
Y_n &:= 3N_n \\
Z_n &:= 3N_n + 1 \\
R_n &:= 9N_n + 3 + 2^{\tau_n} = \mathcal{S}^2(N_n) \cdot 2^{\omega(3\mathcal{S}(N_n)+1)}
\end{aligned}$$

To summarize, we have the following simple identities:

$$Z_n = Y_n + 1 = 2^{\tau_n} \mathcal{S}(N_n) \tag{5.1}$$

$$R_n = 2^{\omega(R_n)} \mathcal{S}^2(N_n) \tag{5.2}$$

5.1. Algorithms and finite-state machines

5.1.1. Algorithm for Y_n. As in Definition 5.0.1, let $N_n = \sum_{i=0}^{n-1} t_i 2^i$ be a number in $\mathbb{N}_{\text{odd}} \cap [1, 2^n - 1]$, expressed as a binary expansion. Then $2N_n = \sum_{i=1}^{n} t_{i-1} 2^i$. If we define the binary sequence $(s_i)_{i=0}^{n+1}$ by

$$Y_n = N_n + 2N_n = \sum_{i=1}^{n+1} s_i 2^i,$$

then $(s_i)_{i=1}^{n+1}$ can be determined by the usual method for adding two numbers digit-by-digit with carries, and in this particular setup the digit-by-digit summations will be of the form $t_i + t_{i-1} + carry$, where *carry* is a variable that assumes the value 0 or 1, according to whether there resulted a carry in adding t_{i-1} and t_{i-2}. We recall this procedure as Algorithm 1 below. An important feature is that after adding the first n digits $t_0, t_1, \ldots, t_{n-1}$ of N_n to the first n digits $0, t_0, t_1, \ldots t_{n-2}$ of $2N_n$ (respectively), it remains to "clear remaining carries," that is, to append two "0" digits to N_n (in the 2^n and 2^{n+1} places) and one "0" digit to $2N_n$ (in the 2^{n+1} place), and then to sum the final two pairs of digits (in the 2^n and 2^{n+1} places) with any carries that remain. This is precisely the base-2 version of the algorithm done in elementary school (where the base is usually 10) in the special case that the two numbers being added are of the form N_n and $2N_n$. We only emphasize the algorithm now because variants of it – Algorithms 2 and 3, which are the important ones for our purposes – will be considered later, and it will be helpful to have this familiar case well in mind.

In all of the pseudocode that follows in this chapter, we write $x\%2 = r$ (for $x \in \mathbb{N}$) to indicate that $r \in \{0, 1\}$ and that $x \equiv r \bmod 2$. We also let $F : \{0, 1, 2, 3\} \to \{0, 1\}$ be the floor function defined by $F(x) = \lfloor x/2 \rfloor$.

Algorithm 1 Base-2 expansion of $Y_n = 3N_n$

1: **input** binary sequence $(1, t_1, t_2, \ldots, t_{n-1})$ ▷ $N_n = 1 + \sum_{i=1}^{n-1} t_i 2^i$
2: $s_0 \leftarrow 1$ ▷ Define $s_0 = 1$, as Y_n is odd.
3: $carry \leftarrow 0$ ▷ Initially there is no carry.
4: **for** $1 \le i \le n-1$ **do**
5:     $s_i \leftarrow (t_i + t_{i-1} + carry)\%2$
6:     $carry \leftarrow F(t_i + t_{i-1} + carry)$
7: **end for**
8: $s_n \leftarrow (t_{n-1} + carry)\%2$ ▷ Remaining carries must be cleared (lines 8-10).
9: $carry \leftarrow F(t_{n-1} + carry)$
10: $s_{n+1} \leftarrow carry\%2$
11: **return** $(s_0, s_1, s_2, \ldots, s_{n+1})$ ▷ $Y_n = 3N_n = \sum_{i=0}^{n-1} s_i 2^i$

Algorithm 1 can be described as a $(n+1)$-step walk on the directed graph shown in Figure 5.1, which has four nodes or *states*. Let us explain the connection. Initially a walker starts at state A. The pair $1/N$ labelling the node A is meant to indicate that $t_0 = 1$ and that no carry is present at the start of the algorithm ("N" for "no carry" – not to be confused with the natural number N_n). The walker's first step depends on t_1, in the following way. If $t_1 = 0$, then the walker moves along the edge labelled $0/1$ to node B. The "0" in the label is the value of t_1, and the "1" in the label is the value of s_1 in the Algorithm 1 for Y_n. Notice that in state B the pair $0/N$ indicates that $t_1 = 0$ and that no carry resulted in adding t_0 and t_1 to obtain s_1. If, on the other hand, $t_1 = 1$, then the walker would move from state A along the edge labelled $1/0$. The "1" is the value of t_1, and the "0" is the value of s_1. In this case a carry results from adding t_0 and t_1, and accordingly state C is labelled with $1/Y$ to indicate that $t_1 = 1$ and that "yes" a carry resulted.

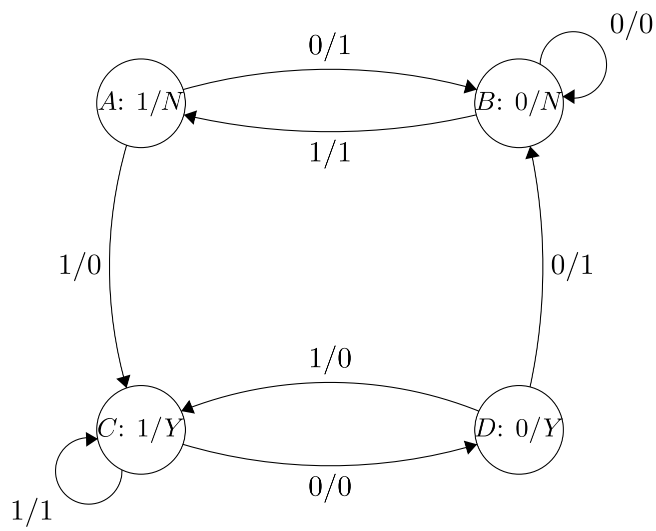


FIGURE 5.1. 4-state machine representing $N_n \mapsto Y_n = 3N_n$ and $N_n \mapsto Z_n = 3N_n + 1$.

So far we have only described the initial step a walker takes and the relationship of this step to t_1 and s_1 as well as the meaning of the labels. But the walker will take $n+1$ steps in total, and the ith step in general corresponds to the declaration of s_i in Algorithm 1. Let us explain this further. Generalizing the labeling scheme above for t_1 and s_1 to t_i and s_i with $i > 1$, we will interpret labels above edges as *input/output* pairs, with the *input* being t_i and the *output* being s_i; and we will interpret the label of the ith state as indicating the value of t_i and the current value of the variable *carry*, which is the binary value of the carry that results in adding t_{i-1}, t_i, and the previous carry. Example 5.1.1 below may further clarify. Starting from state A, the walker will take a sequence of $n-1$ steps – corresponding to the for-loop in Algorithm 1 (lines 4-7) – moving on the ith step to the state connected to the walker's current state by the directed edge having t_i (the input) as the first entry in its label. The second entry (the output) is s_i.

To finish, the walker takes two more steps, which correspond to *clearing remaining carries* in lines 8-10 of Algorithm 1. Specifically, on the nth step the walker moves from its current state to a new state along the edge having 0 as the first entry in its label. In other words, we force the input to be 0. The output gives the value of s_n. On the $(n+1)$th step the walker again moves from its current state along the edge having 0 as the first entry. The output again defines s_{n+1}, and the walker will invariably arrive at state B.

EXAMPLE 5.1.1. If $n = 4$ and $N_n = 13$, then $(t_0, t_1, t_2, t_3) = (1, 0, 1, 1)$. Starting at state A, the walker in Figure 5.1 visits the nodes B, A, C, D, B, in order, with outputs respectively of $1, 1, 0, 0, 1$, which correspond to the values of s_1, s_2, s_3, s_4, s_5 in Algorithm 1. Since $s_0 = 1$, we have $Y_n = 1 + 2 + 4 + 32 = 39$.

A directed graph such as the one we have constructed – that models a computational algorithm by finitely many states, with transitions that depend on a sequence of input data – is often referred to as a *finite-state machine* (or *finite-state automaton*). For more information, one can consult a standard introductory textbook on applied discrete mathematics or computation theory (e.g. [**Woo86**]).

5.1.2. Algorithm for Z_n. Now we slightly modify the previous algorithm in order to compute $Z_n = 3N_n + 1$, where $N_n = \sum_{i=0}^{n-1} t_i 2^i \in \mathbb{N}_{\text{odd}} \cap [1, 2^n - 1]$, with $t_0 = 1$ as before. We write $Z_n = \sum_{s=0}^{n+1} s_i 2^i$ as the binary expansion, using the same symbols (s_i) as we did for Y_n in order to emphasize that Algorithm 2 is exactly the same as Algorithm 1, except for two changes in initial conditions. In particular, we initialize s_0 with the value 0 (not 1), as Z_n is an even number. Moreover, as $Z_n = Y_n + 1$ and we already have Algorithm 1 for Y_n, we can achieve the extra "+1" by running Algorithm 1 and simply initializing the carry to have the value $carry = 1$ (instead of 0). The result is Algorithm 2 below, which is identical to Algorithm 1 except for these changes in lines 2 and 3 and the interpretation of the returned value (colored in blue).

Algorithm 2 Base-2 expansion of $Z_n = 3N_n + 1$

1: **input** binary sequence $(1, t_1, t_2, \dots, t_{n-1})$ $\qquad \triangleright\ N_n = 1 + \sum_{i=1}^{n-1} t_i 2^i$
2: $s_0 \leftarrow 0$ $\qquad \triangleright$ Define $s_0 = 0$, as Z_n is odd.
3: $carry \leftarrow 1$ $\qquad \triangleright$ Initialize the carry as 1.
4: **for** $1 \le i \le n-1$ **do**
5: $\quad s_i \leftarrow (t_i + t_{i-1} + carry)\%2$
6: $\quad carry \leftarrow F(t_i + t_{i-1} + carry)$
7: **end for**
8: $s_n \leftarrow (t_{n-1} + carry)\%2$ $\qquad \triangleright$ Remaining carries must be cleared (lines 8-10).
9: $carry \leftarrow F(t_{n-1} + carry)$
10: $s_{n+1} \leftarrow carry\%2$
11: **return** $(s_0, s_1, s_2, \dots, s_{n+1})$ $\qquad \triangleright\ Z_n = 3N_n + 1 = \sum_{i=0}^{n-1} s_i 2^i$

In terms of the finite-state machine in Figure 5.1, the change of initial conditions that differentiates Algorithm 2 from Algorithm 1 translates to the walker for this model of Z_n beginning its journey in state C, not in state A as before. The rest of the walk proceeds with the same rules, including for the last two steps, for which the input is 0 (clearing remaining carries). The walker invariably ends in state B, as before.

Example 5.1.2. If $n = 5$ and $N_n = 19$, then $(t_0, t_1, t_2, t_3, t_4) = (1, 1, 0, 0, 1)$. Starting at state C the walker in Figure 5.1 visits the nodes C, D, B, B, A, B, B, in order, with outputs respectively of $1, 0, 1, 1, 1, 0$ which correspond to the values of $s_1, s_2, s_3, s_4, s_5, s_6$ in Algorithm 2. Since $s_0 = 0$, we have $Z_n = 2 + 8 + 16 + 32 = 58$.

5.1.3. Algorithm for R_n. The 4-state machine introduced above was a model for algorithms that compute the values $Y_n = 3N_n$ and $Z_n = 3N_n + 1$, or, more precisely, their sequences of binary digits. Each digit t_i of N_n acts as an input that results in the ith step of the machine or algorithm. In this section we present Algorithm 3 (below) and an associated 16-state machine, which produce the analogous sequence of outputs in the operation $N_n \mapsto R_n = 9N_n + 3 + 2^{\tau_n}$. That is, the algorithm produces the vector of binary digits $(r_0, r_1, \dots, r_{n+3})$ of $R_n = \sum_{i=1}^{n+3} r_i 2^i$.

To introduce the procedure, let us suggest that in ignoring all references to the sequence $(r_i)_{i=0}^{n+3}$ in the psuedocode of Algorithm 3, the reader will see that Algorithm 3 reduces to Algorithm 2 for the sequence $(s_i)_{i=0}^{n+1}$ of binary digits in Z_n in the specific case that Z_n is not a power of 2 (which is precisely the case in which the if-condition is false in lines 2-3 of Algorithm 3). In particular, as i ranges over $\{1, 2, \dots, \tau_n\}$ in the for-loop in lines 5-8 of Algorithm 3, the same values of s_i are produced as are produced as i ranges over the same set in the for-loop in lines 4-7 of Algorithm 2, namely $s_i \equiv 0$. Then, as i ranges over $\{\tau_n, \tau_n + 1, \ldots, n-1\}$ in lines 13-18 of Algorithm 3, the same values of s_i are produced as are produced when i ranges over the same set in lines 5-8 of Algorithm 2; and moreover, the exact same procedure involving carries is used in both cases. After that, the clearing of the carries is done exactly the same way in both algorithms, with $carry_1$ in Algorithm 3 playing the role that $carry$ played in Algorithm 2. One might therefore argue that with respect to the sequence $(s_i)_{i=0}^{n+1}$, the only difference between the two algorithms is in how they produce the initial string of τ_n "0"s in the sequence of binary digits of Z_n. In some sense then, Algorithm 2 is redundant. But it seems reasonable to isolate the computation of Z_n, as we will specifically rely on it later, and to also gradually lead the reader into an understanding of

---

Algorithm 3 Base-2 expansion of $R_n = 9N_n + 3 + 2^{\tau_n}$

1: **input** binary sequence $(1, t_1, t_2, \ldots, t_{n-1})$ ▷ $N_n = 1 + \sum_{i=1}^{n-1} t_i 2^i$
2: **if** $\tau_n \geq n$ **or** $t_i = 0$ for $i \geq \tau_n$ **then**
3:     **return** $(\overbrace{0, 0, \ldots, 0}^{\tau_n+1 \text{ times}}, 1)$ ▷ $9N_n + 3 + 2^{\tau_n} = 2^{\tau_n+2}$
4: **end if**
5: **for** $0 \leq i < \tau_n$ **do**
6:     $s_i \leftarrow 0$
7:     $r_i \leftarrow 0$
8: **end for**
9: $s_{\tau_n} \leftarrow 1$
10: $r_{\tau_n} \leftarrow 0$
11: $carry_1 \leftarrow \tau_n \% 2$
12: $carry_2 \leftarrow 1$
13: **for** $\tau_n < i \leq n-1$ **do**
14:     $s_i \leftarrow (t_i + t_{i-1} + carry_1)\%2$
15:     $carry_1 \leftarrow F(t_i + t_{i-1} + carry_1)$
16:     $r_i \leftarrow (s_i + s_{i-1} + carry_2)\%2$
17:     $carry_2 \leftarrow F(s_i + s_{i-1} + carry_2)$
18: **end for**
19: $s_n \leftarrow (t_{n-1} + carry_1)\%2$ ▷ Lines 19-28 are clearing the carries.
20: $carry_1 \leftarrow F(t_{n-1} + carry_1)$
21: $r_n \leftarrow (s_n + s_{n-1} + carry_2)\%2$
22: $carry_2 \leftarrow F(s_n + s_{n-1} + carry_2)$
23: $s_{n+1} \leftarrow carry_1 \% 2$
24: $r_{n+1} \leftarrow (s_{n+1} + s_n + carry_2)\%2$
25: $carry_2 \leftarrow F(s_{n+1} + s_n + carry_2)$
26: $r_{n+2} \leftarrow (s_{n+1} + carry_2)\%2$
27: $carry_2 \leftarrow F(s_{n+1} + carry_2)$
28: $r_{n+3} \leftarrow carry_2 \% 2$
29: **return** $(r_0, r_1, r_2, \ldots, r_{n+3})$ ▷ $R_n = \sum_{i=0}^{r+3} r_i 2^i$

Algorithm 3, which at first glance might appear to be much more involved than the previous two, but is actually quite natural.

Computationally, the upshot of Algorithm 3 regards the sequence $(r_i)_{i=0}^{n+3}$. Indeed, for $1 \leq i \leq n+1$, the value r_i is produced in the algorithm as soon as s_i is produced (i.e. in the same step of a for-loop or in the formal sense that r_i is a function of s_i, s_{i-1}, and the two carries involved, as we explain in more detail below). Therefore r_i is known as soon as $\{t_k : k \leq i\}$ is known. This will be useful later when we consider r_i – as a random variable – to be a deterministic function of the random binary vector $(t_0, t_1, \ldots, t_i)$.

The reader is invited to work through the pseudocode, or to use the SAGE implementation provided in Figure 5.3. We explain the recursive mechanism at work. The key observation from arithmetic is that if $N_n = \sum_{i=0}^{\infty} t_i 2^i$ is an odd number written in binary, then in order to determine the binary digit s_k in the expansion $Z_n = 3N_n + 1 = \sum_{i=0}^{\infty} s_i 2^i$, it is sufficient to know t_k, t_{k-1}, and whether a carry resulted when adding t_{k-1}, t_{k-2}, and any inherited carry from prior steps. Indeed this is the underlying idea for the 4-state model. Similarly, in the expansion $R_n = 3Z_n + 2^{\tau_n} = \sum_{i=0}^{\infty} r_i 2^i$, we see that r_k can determined if we know s_k, s_{k-1}, and whether a carry resulted from adding s_{k-1} and s_{k-2}. Thus, the following four data points determine the value of r_k, given the input t_k:

(1) t_{k-1}
(2) binary value of carry resulting from $t_{k-1} + t_{k-2}$ (+ any inherited carry)
(3) s_{k-1}
(4) binary value of carry resulting from $s_{k-1} + s_{k-2}$ (+ any inherited carry)

Furthermore, upon receiving the input t_k, one can obviously determine from the latter quadruple of information – which we refer to as the $(k-1)$th *state* – the subsequent quadruple of information – which defines the kth state – namely:

(1) t_k
(2) binary value of carry resulting from $t_k + t_{k-1}$ (+ any inherited carry)
(3) s_k
(4) binary value of carry resulting from $s_k + s_{k-1}$ (+ any inherited carry)

Thus, each such quadruple of information can be viewed as a a node in a directed graph from which we pass to another node upon knowing a new digit in the sequence (t_i). Algorithm 3 formalizes this process, with $carry_1$ and $carry_2$ keeping track of the carries involved in adding values

FIGURE 5.2. Connectivity of the 16-state machine for Algorithm 3

	(0,N,0,N)	(0,N,0,Y)	(0,N,1,N)	(0,N,1,Y)	(0,Y,0,N)	(0,Y,0,Y)	(0,Y,1,N)	(0,Y,1,Y)	(1,N,0,N)	(1,N,0,Y)	(1,N,1,N)	(1,N,1,Y)	(1,Y,0,N)	(1,Y,0,Y)	(1,Y,1,N)	(1,Y,1,Y)
(0,N,0,N)	**0/0**										**1/1**					
(0,N,0,Y)	**0/1**											**1/1**				
(0,N,1,N)	**0/1**											**1/0**				
(0,N,1,Y)		**0/0**										**1/1**				
(0,Y,0,N)			**0/1**										**1/0**			
(0,Y,0,Y)				**0/0**									**1/1**			
(0,Y,1,N)				**0/0**									**1/1**			
(0,Y,1,Y)				**0/1**										**1/0**		
(1,N,0,N)			**0/1**										**1/0**			
(1,N,0,Y)				**0/0**									**1/1**			
(1,N,1,N)				**0/0**									**1/1**			
(1,N,1,Y)				**0/1**										**1/1**		
(1,Y,0,N)					**0/0**										**1/1**	
(1,Y,0,Y)					**0/1**											**1/0**
(1,Y,1,N)					**0/1**											**1/0**
(1,Y,1,Y)						**0/0**										**1/1**

of (t_i) and (s_i), respectively. There are at most 16 possible states a walker can reach, depending on the binary values of the components of the quadruple. We can represent these states in a finite-state machine, as we did for Y_n and Z_n. Rather than illustrate the machine with a graph, we describe its connectivity in the form of a matrix (see Figure 5.2), according to the following rule. The presence of a specific *input/output* pair t_k/r_k in the ith row and jth column of the matrix has the following significance: if just after the $(k-1)$th step the machine is in the state that labels the ith row, and the input received is t_k, then the new (kth) state is that which labels the jth column, and the output is r_k. On the other hand, if the entry in the ith row and jth column is empty, then there is no directed edge from the state that labels the ith row to the state that labels the jth column. The symbols N and Y stand for "no carry" and "yes carry," as before. For example, if the kth state of the machine is $(1, N, 0, Y)$, then we would interpret that $t_k = 1$ and $carry_1 = 0$ (so no carry results in adding t_k and t_{k-1}), while $s_k = 0$ and $carry_2 = 1$ (so a carry does result in adding s_k and s_{k-1}).

The reader will see that the information encoded by the matrix in Figure 5.2 agrees with the recursive rule that we explained above to determine r_k and $(t_k, carry_1, s_k, carry_2)$ from $(t_{k-1}, carry_1, s_{k-1}, carry_2)$ and t_k.

EXAMPLE 5.1.3. Consider the following data points for the kth state of the machine:

(1) $t_k = 0$,
(2) binary value of the carry resulting from $t_k + t_{k-1}$ is 0, or N for "no carry" ,
(3) $s_k = 1$,
(4) binary value of the carry resulting from $s_k + s_{k-1}$ is 1, or Y for "yes carry" .

We represent this state as the tuple $(0, N, 1, Y)$. A walker would move from $(0, N, 1, Y)$ to $(0, N, 0, Y)$ upon receiving an input of $t_{k+1} = 0$, and the result would be an output of $r_{k+1} = 0$;

FIGURE 5.3. SAGE implementation of Algorithm 3

```
def tau(N,n):                       ### FUNCTION: tau(N,n)
    v=N.digits(2)                   ### INPUT: (N,n)
    for j in range(n-len(v)):        ## n is a positive integer.
        v.append(0)                  ## N is a positive odd integer less than 2^n.
    for i in [1..len(v)-1]:         ### OUTPUT: base-2 valuation of 3N+1
        if v[i]==v[i-1]:
            return i
    if v[n-1]==0:
        return n                    ### FUNCTION: alg3(N,n)
    else:                           ### INPUT: (N,n)
        return n+1                   ## n is a positive integer.
                                     ## N is a positive odd integer less than 2^n.
                                    ### OUTPUT: (r,R)
                                     ## R=9N+3+2^{tau(N,n)}.
                                     ## r=[0,r_1,...,r_{n+3}], list of digits of R.
                                     ## R=sum_{i=0}^{n+3}(r_i 2^i).


def alg3(N,n):
    v=N.digits(2)
    for j in range(n-len(v)):
        v.append(0)
    T=tau(N,n)
    if T>=n or sum([v[i] for i in [T..(n-1)]])==0:
        L=[0]
        for i in range (0,T+1):
            L.append(0)
        L.append(1)
        return (L, sum([L[i]*2^i for i in [0..(T+2)]]))
    s=[]
    r=[]
    for i in [0..T-1]:
        s.append(0)
        r.append(0)
    r.append(0)
    s.append(1)
    carry1=T%2
    carry2=1
    for i in [T+1..n-1]:
        s.append((v[i]+v[i-1]+carry1)%2)
        carry1=floor((v[i]+v[i-1]+carry1)/2)
        r.append((s[i]+s[i-1]+carry2)%2)
        carry2=floor((s[i]+s[i-1]+carry2)/2)
    s.append((v[n-1]+carry1)%2)
    carry1=floor((v[n-1]+carry1)/2)
    r.append((s[n]+s[n-1]+carry2)%2)
    carry2=floor((s[n]+s[n-1]+carry2)/2)
    s.append(carry1%2)
    r.append((s[n+1]+s[n]+carry2)%2)
    carry2=floor((s[n+1]+s[n]+carry2)%2)
    r.append((s[n+1]+carry2)%2)
    carry2=floor((s[n+1]+carry2)/2)
    r.append(carry2%2)
    return (r, sum([r[i]*2^i for i in [0..(n+3)]]))
```

the walker would instead move to $(1, N, 1, Y)$ with an input of $t_{k+1} = 1$, and the output would be $r_{k+1} = 1$

There is more to be said about using the 16-state machine to determine $\sigma(R_n)$, since we have so far only explained the recursive part – the steps between nodes – but not the initial condition, i.e. the starting node of the walk. The details will be important later in the random setting. Looking at Algorithm 3 in either the pseudocode or the SAGE code, one observes that the first step is to determine τ_n. If $\tau_n \geq n$, or if $t_i = 0$ for $i \geq \tau_n$, then R_n is a power of 2, and $\sigma(R_n) = 1$. When R_n is not a power of 2, the procedure for defining r_i for $1 \leq i \leq \tau_n$ is trivial, namely $r_i \equiv 0$. After that, if τ_n is *even*, then $t_{\tau_n} = 0, carry_1 = 0, s_{\tau_n} = 1$, and $carry_2 = 1$, so the walker starts at $(0, N, 1, Y)$. On the other hand, if τ_n is *odd*, then $t_{\tau_n} = 1, carry_1 = 1, s_{\tau_n} = 1$, and $carry_2 = 1$, so the walker starts instead at $(1, Y, 1, Y)$. In either case, the walker will take the next $n - 1 - \tau_n$ steps according to the values of $(t_i)_{i=\tau_{n+1}}^{n-1}$. After completing these $n - 1 - \tau_n$ steps, the walker must clear remaining carries by taking four final steps, each with input 0, and will invariably arrive at state $(0, N, 0, N)$. We will discuss this last part more in more detail in the random setting below.

5.2. Proof of Theorem 1.5.2

5.2.1. Random binary vectors and a preliminary lemma. As a preliminary step, we set up a simple correspondence between random numbers and random binary vectors by identifying N_n and $\mathcal{S}(N_n)$ with the lists of digits in their respective binary expansions. Thus, we let $(t_n)_{n=1}^{\infty}$ be an infinite sequence of i.i.d. Bernoulli(1/2) random variables, and for each $n \geq 1$ we make the identification

$$N_n = \left(\sum_{i=0}^{n-1} t_i 2^i \right) \mapsto (t_0, t_1, \dots t_{n-1}),$$

with $t_0 = 1$. It is clear that this is a bijection with n-tuples of binary vectors having $t_0 = 1$, and that the probability measure on $\mathbb{N}_{\text{odd}} \cap [1, 2^n - 1]$ is uniform with either interpretation of N_n.

In the next lemma we reduce the of proof Theorem 1.5.2 to the evaluation of $\mathbb{E}(\sigma(Z_n))$.

Lemma 5.2.1. *To prove Theorem* (1.5.2)*, it suffices to prove that*

$$\mathbb{E}(\sigma(Z_n)) = \frac{n}{2} + \frac{1}{6} + \frac{3 + (-1)^n}{3 \times 2^n}. \tag{5.3}$$

Proof. From (5.1), we see that $\sigma(Z_n) = \sigma(\mathcal{S}(N_n))$, so that recalling Definition 1.5.4 we may write

$$D_n = \mathbb{E}(\sigma(N_n)) - \mathbb{E}(\sigma(Z_n))\,. \tag{5.4}$$

Since $t_0 = 1$, we have

$$\mathbb{E}(\sigma(N_n)) = 1 + \left(\sum_{i=1}^{n-1} \mathbb{E}t_i\right) = \frac{n}{2} + \frac{1}{2}.$$

The validity of (5.3) would then imply by (5.4) that

$$D_n = \frac{n}{2} + \frac{1}{2} - \left(\frac{n}{2} + \frac{1}{6} + \frac{3 + (-1)^n}{3 \times 2^n}\right) = \frac{1}{3} - \frac{3 + (-1)^n}{3 \times 2^n}\,,$$

which is the desired conclusion. □

In view of the correspondence between random numbers N_n and random vectors $(t_0, t_1, \ldots, t_{n-1})$ as well as Algorithm 2 and its connection to the 4-state machine, we can think of $\mathbb{E}(\sigma(Z_n))$ as the expectation of the sum of outputs of a random walker on the 4-state machine, whose steps are determined by the random binary numbers $(t_i)_{i=0}^{\infty}$. In the next section we will make this more precise and compute $\mathbb{E}(\sigma(Z_n))$.

5.2.2. 4-state recurrence. We introduce some new definitions. These really amount simply to new notation for various features of the algorithms discussed above, translated to the random setting.

Definition 5.2.1. For $n > 0$, let $W_n(A)$ denote the location of a random walker in the 4-state machine who starts at node A and walks for $n-1$ steps, according to the values of the random inputs $(t_i)_{i=1}^{n-1}$ in the manner described above regarding edge labels. Similarly, define $W_n(B), W_n(C)$, and $W_n(D)$ to be the final locations for the random walker who starts at nodes B, C, and D, respectively.

For example, $W_1(A) = A$, and similarly for B, C, and D. $W_2(A)$ takes the values B and C with probabilities $1/2$ each, and $W_3(A)$ is uniformly distributed over $\{A, B, C, D\}$. In general, at the ith step the random walker crosses to one of two nodes with probabilities $1/2$ each – according to the value of t_i – and arrives at the $(i+1)$th node of the walk (including the starting node). Toward illustrating these concepts further, one may verify the following identity:

$$P(W_n(A) = C) = \frac{1}{2}P(W_{n-1}(A) = A) + \frac{1}{2}P(W_{n-1}(A) = C) + \frac{1}{2}P(W_{n-1}(A) = D)\,.$$

DEFINITION 5.2.2. Define four sequences of random variables $(A_n)_{n=1}^{\infty}, (B_n)_{n=1}^{\infty}, (C_n)_{n=1}^{\infty}$, and $(D_n)_{n=1}^{\infty}$ as follows. A_n is the sum of outputs of all edges traversed by a random walker who starts at node A and walks for $n-1$ steps according to the random inputs $(t_i)_{i=1}^{n-1}$. The other sequences are defined analogously for the random walker starting at B, C, or D.

Comparing with the algorithms above one sees that A_n and C_n are the random versions of the sums $\sum_{i=1}^{n-1} s_i$, with $(s_i)_{i=1}^{n-1}$ as in Algorithms 1 and 2, respectively.

DEFINITION 5.2.3. Define four sequences of *residues* – $(resA_n)_{n=1}^{\infty}, (resB_n)_{n=1}^{\infty}, (resC_n)_{n=1}^{\infty}$, and $(resD_n)_{n=1}^{\infty}$ – as follows. From the node $W_n(A)$, find the edge with input 0. Traverse this edge to arrive at a node, which is the walker's nth state. From this node, find the edge with input 0, and traverse this edge, arriving invariably at the node B. Add up the outputs of both of the edges traversed in this process. This number by definition is $resA_n$. The other sequences of residues are defined analogously in terms of $W_n(B)$, $W_n(C)$, and $W_n(D)$. Observe that each residue is 0 or 1.

For example, $resA_n$ (resp. $resC_n$) is precisely the value of s_n+s_{n+1} from the "clearing remaining carries" part (lines 8-10) of Algorithm 1 (resp. 2) for a random input sequence $(t_i)_{i=1}^{n-1}$.

DEFINITION 5.2.4. Define four sequences $(\alpha_n)_{n=1}^{\infty}, (\beta_n)_{n=1}^{\infty}, (\gamma_n)_{n=1}^{\infty}$, and $(\delta_n)_{n=1}^{\infty}$, and a sequence of vectors $(v_n)_{n=1}^{\infty}$, by

$$\alpha_n = \mathbb{E}(A_n + resA_n), \qquad \beta_n = \mathbb{E}(B_n + resB_n),$$

$$\gamma_n = \mathbb{E}(C_n + resC_n), \qquad \delta_n = \mathbb{E}(D_n + resD_n),$$

and $v_n = (\alpha_n, \beta_n, \gamma_n, \delta_n)$.

LEMMA 5.2.2. $\mathbb{E}(\sigma(Z_n)) = \gamma_n$

PROOF. This is just a matter of tracking the definitions. Indeed both the left and right sides of the equation are equal to $\sum_{i=0}^{n+1} s_i$, where $(s_i)_{i=0}^{n+1}$ is the output of Algorithm 2 in the case of a random input $(t_i)_{i=1}^{n-1}$ (and $t_0 = 1$). □

Lemma 5.2.3. *In addition to the initial value* $v_1 = (1, 0, 1, 1)$*, we have the following recurrence relation for* $(v_n)_{n=1}^{\infty}$*. For* $n > 0$*,*

$$\alpha_n = \frac{1}{2}(\beta_{n-1} + 1) + \frac{1}{2}\gamma_{n-1}\,,$$
$$\beta_n = \frac{1}{2}(\alpha_{n-1} + 1) + \frac{1}{2}\beta_{n-1}\,,$$
$$\gamma_n = \frac{1}{2}(\gamma_{n-1} + 1) + \frac{1}{2}\delta_{n-1}\,,$$
$$\delta_n = \frac{1}{2}(\beta_{n-1} + 1) + \frac{1}{2}\gamma_{n-1}\,.$$

More concisely, letting x^* *denote the transpose of a vector* $x = (x_1, x_2, x_3, x_4)$*, we have*

$$v_n = Sv_{n-1}^* + c, \tag{5.5}$$

where $c = \left(\frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}\right)$*,* $S = \begin{pmatrix} 0 & \frac{1}{2} & \frac{1}{2} & 0 \\ \frac{1}{2} & \frac{1}{2} & 0 & 0 \\ 0 & 0 & \frac{1}{2} & \frac{1}{2} \\ 0 & \frac{1}{2} & \frac{1}{2} & 0 \end{pmatrix}$*, and the multiplication in (5.7) is of matrices.*

Proof. The value of w_1 follows directly from Definition 5.2.4. The recurrence relation follows from the connectivity of the 4-state machine in Figure 5.1, linearity of expectation, Definitions 5.2.1 - 5.2.4, and the probability distribution on $(t_i)_{i=1}^{\infty}$. □

Now we will complete the proof of Theorem 1.5.2 by verifying the identity (5.3) in Lemma 5.2.1.

Proposition 5.2.1. *The identity (5.3) is valid, i.e.*

$$\mathbb{E}(\sigma(Z_n)) = \frac{n}{2} + \frac{1}{6} + \frac{3 + (-1)^n}{3 \times 2^n}\,.$$

Proof. By Lemma 5.2.2 it suffices to show that γ_n has the value on the right side of the latter identity. We will do this by solving for γ_n in the recurrence relation of Lemma 5.3.2. This recurrence can be solved exactly. The vector c is fixed by S, so the recurrence gives the following expression for v_n, $n > 1$:

$$\begin{aligned} v_n &= S^{n-1}v_1 + S^{n-2}c + S^{n-3}c + \cdots + S^2c + Sc + c \\ &= S^{n-1}v_1 + (n-1)c\,. \end{aligned}$$

As S is diagonalizable, it is routine to compute that $S^{n-1}v_1 = \begin{pmatrix} \frac{2}{3} + \frac{1}{3}\left(-\frac{1}{2}\right)^{n-1} \\ \frac{2}{3} - \left(\frac{1}{2}\right)^n + \frac{1}{3}\left(-\frac{1}{2}\right)^n \\ \frac{2}{3} + \left(\frac{1}{2}\right)^n + \frac{1}{3}\left(-\frac{1}{2}\right)^n \\ \frac{2}{3} + \frac{1}{3}\left(-\frac{1}{2}\right)^{n-1} \end{pmatrix}$.

With $\cdot$ denoting the vector dot product, we thus obtain

$$\begin{aligned} \gamma_n &= (S^{n-1}v_1 + (n-1)c) \cdot (0,0,1,0) \\ &= \frac{2}{3} + \left(\frac{1}{2}\right)^n + \frac{1}{3}\left(-\frac{1}{2}\right)^n + \frac{n-1}{2} \\ &= \frac{n}{2} + \frac{1}{6} + \frac{3+(-1)^n}{3 \times 2^n}, \end{aligned}$$

and the proposition follows. □

5.3. Proof of Theorem 1.5.3

Our approach here is the same in principle as in the proof of Theorem 1.5.2, but with more complicated technical details. In particular we start with a reduction of the problem, similar to Lemma 5.2.1.

LEMMA 5.3.1. *To prove Theorem 1.5.3, it suffices to prove that*

$$\mathbb{E}(\sigma(R_n)) = \frac{n+1}{2} - \frac{5}{9} + \frac{b_n}{9 \times 2^{n-1}} \tag{5.6}$$

PROOF. Recalling Definition 1.5.4 and comparing with (1.26), the lemma follows directly from the fact that $\mathbb{E}(\sigma(N_n)) = (n+1)/2$ and from (5.2), which implies that $\mathbb{E}(\sigma(\mathcal{S}^2(n))) = \mathbb{E}(\sigma(R_n))$. □

In order to verify (5.6), we will first establish a recurrence relation for the 16-state machine depicted in Figure 5.2. Then we will partition the probability space of possible values of R_n, according to the value of τ_n. After that we will compute the conditional expectations of $\sigma(R_n)$

with respect to this partition, using the recurrence relation for the 16-state machine. To conclude we will apply the law of total expectation to evaluate $\mathbb{E}(\sigma(R_n))$.

5.3.1. 16-state recurrence. We introduce some new definitions, which amount to new notation for various features of Algorithm 3 that we have already discussed, translated to the random setting. These are analogous to Definitions 5.2.1 - 5.2.4 for the 4-state machine.

DEFINITION 5.3.1. For $i = 1, 2, \ldots, 16$, consider the matrix in Figure 5.2 and let $A^{(i)}$ denote the ith state in the list of states that label the rows, from top to bottom (or, equivalently, the list of states that label the columns from left to right).

For example, $A^{(1)} = (0, N, 0, N)$, $A^{(4)} = (0, N, 1, Y)$, and $A^{(16)} = (1, Y, 1, Y)$.

DEFINITION 5.3.2. For $n > 0$ and $1 \leq i \leq 16$, let $V_n(A^{(i)})$ denote the location of a random walker in the 16-state machine who starts at node $A^{(i)}$ and walks for $n-1$ steps, according to the values of the random inputs $(t_i)_{i=1}^{n-1}$ in the manner described above regarding edge labels.

DEFINITION 5.3.3. Define sixteen sequences of random variables $(A_n^{(i)})_{n=1}^{\infty}$ $(1 \leq i \leq 16)$ as follows. $A_n^{(i)}$ is the sum of outputs of all edges traversed by a random walker who starts at node $A^{(i)}$ and walks for $n-1$ steps according to the random inputs $(t_i)_{i=1}^{n-1}$.

DEFINITION 5.3.4. Define sixteen sequences of *residues* $(resA_n^{(i)})_{n=1}^{\infty}(1 \leq i \leq 16)$ as follows. From the node $V_n(A^{(i)})$, find the edge with input 0. Traverse this edge to arrive at a node, which is the walker's nth state. From this node, find the edge with input 0, and traverse this edge, arriving at the walker's $(n+1)$th state. Do this twice more, invariably arriving at the node $A^{(1)}$, which is the $(n+3)$th state. Add up the outputs of the four edges traversed in this process. This number by definition is $resA_n^{(i)}$. The other sequences of residues are defined analogously for $2 \leq i \leq 16$. Observe that each residue is among the set $\{0, 1, 2, 3\}$.

DEFINITION 5.3.5. Define for $i = 1, 2, \ldots, 16$ the sequence $(\alpha_n^{(i)})_{n=1}^{\infty}$, by

$$(\alpha_n^{(i)})_{n=1}^{\infty} = (\mathbb{E}(A_n^{(i)} + resA_n^{(i)}))_{n=1}^{\infty}.$$

Also, define the vector w_n by

$$w_n = (\alpha_n^{(1)}, \alpha_n^{(2)}, \ldots, \alpha_n^{(16)}).$$

LEMMA 5.3.2. *In addition to the initial value*

$$\begin{aligned} w_1 &= (\alpha_1^{(1)}, \alpha_1^{(2)}, \ldots, \alpha_1^{(16)}) \\ &= (0,1,1,1,2,1,1,2,2,1,1,2,2,3,3,1) \end{aligned}$$

the following recurrence relation holds for $(w_n)_{n=1}^{\infty}$. *For* $n > 0$, *letting* x^* *denote the transpose of a vector* $x = (x_1, x_2, \ldots, x_{16})$, *we have*

$$w_n = Tw_{n-1}^* + d, \tag{5.7}$$

where d *is the* 16*-tuple with* 1/2 *in every coordinate, and*

$$T = \begin{pmatrix}
\frac{1}{2} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{2} & 0 & 0 & 0 & 0 & 0 \\
\frac{1}{2} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{2} & 0 & 0 & 0 & 0 \\
\frac{1}{2} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{2} & 0 & 0 & 0 & 0 \\
0 & \frac{1}{2} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{2} & 0 & 0 & 0 & 0 \\
0 & 0 & \frac{1}{2} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{2} & 0 & 0 & 0 \\
0 & 0 & 0 & \frac{1}{2} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{2} & 0 & 0 & 0 \\
0 & 0 & 0 & \frac{1}{2} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{2} & 0 & 0 & 0 \\
0 & 0 & 0 & \frac{1}{2} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{2} & 0 & 0 \\
0 & 0 & \frac{1}{2} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{2} & 0 & 0 & 0 \\
0 & 0 & 0 & \frac{1}{2} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{2} & 0 & 0 & 0 \\
0 & 0 & 0 & \frac{1}{2} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{2} & 0 & 0 & 0 \\
0 & 0 & 0 & \frac{1}{2} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{2} & 0 & 0 \\
0 & 0 & 0 & 0 & \frac{1}{2} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{2} & 0 \\
0 & 0 & 0 & 0 & \frac{1}{2} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{2} \\
0 & 0 & 0 & 0 & \frac{1}{2} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{2} \\
0 & 0 & 0 & 0 & 0 & \frac{1}{2} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{2}
\end{pmatrix}$$

PROOF. The value of w_1 follows directly from Definition 5.2.4. The recurrence relation follows from the connectivity of the 16-state machine in Figure 5.2, linearity of expectation, Definitions 5.3.1 - 5.3.5, and the probability distribution on $(t_i)_{i=1}^{\infty}$. $\square$

5.3.2. A partition of the probability space. For $1 \le k \le n+1$, define the events E_k by

$$E_k = \{3N_n + 1 \equiv 2^k (\bmod 2^{k+1})\} = \{\tau_n = k\},$$

in the probabilist's usual event notation that omits reference to the underlying probability space. Equivalently,

$$E_k = \{Z_n = (z_0 = 0, 0, \ldots, 0, z_k = 1, z_{k+1}, \ldots, z_{n+1})\},$$

or likewise

$$E_k = \{\inf\{i : t_i = t_{i-1}\} = k\},$$

where $N_n = \sum_{i=0}^{\infty} t_i 2^i$. It is routine to verify that we have the following probabilities for E_k, $1 \leq k \leq n+1$:

$$P(E_k) = \begin{cases} 2^{-k} & \text{if } 1 \leq k \leq n-1 \\ 2^{-(n-1)} & \text{if } k = n \text{ and } n \text{ even} \\ 0 & \text{if } k = n+1 \text{ and } n \text{ even} \\ 2^{-(n-1)} & \text{if } k = n+1 \text{ and } n \text{ odd} \\ 0 & \text{if } k = n \text{ and } n \text{ odd} \\ 0 & \text{if } k > n+1 \end{cases} \tag{5.8}$$

$$= \begin{cases} 2^{-k} & \text{if} \quad 1 \leq k < n \\ 2^{-n}[1 + (-1)^k] & \text{if} \quad k \in \{n, n+1\} \\ 0 & \text{if} \quad k > n+1 \end{cases}$$

Moreover, the E_k's partition the probability space, i.e. $P(\cup_{k=1}^{n+1} E_k) = 1$, and $E_k \cap E_j = \emptyset$ for $k \neq j$.

5.3.3. Conditional expectations. We determine the conditional expectations $\mathbb{E}(\sigma(R_n)|E_k)$ by considering three cases, namely whether $k \in \{n, n+1\}$, $k < n$ is even, or $k < n$ is odd.

5.3.3.1. *Trivial case:* $k \in \{n, n+1\}$. In this case it is guaranteed that $\mathcal{S}(N_n) = 1$ so that $R_n = 4$, and hence

$$\mathbb{E}(\sigma(R_n)|E_k) = 1\,. \tag{5.9}$$

5.3.3.2. *Even case:* $1 \leq k < n$, *k even.* Assume the event E_k, with even $k < n$. Then the walker starts in state $A^{(4)}$, as explained in the paragraph after Example 5.1.3, and walks for $n-k-1$

steps before taking four final steps to clear carries (as discussed in Section 5.1.3). Therefore,

$$\begin{aligned}
\mathbb{E}(\sigma(R_n)|E_k) &= \alpha^{(4)}_{n-k} \\
&= (T^{n-k-1}v_1 + (n-k-1)d) \cdot (0,0,0,1,0\dots,0,0) \\
&= \left[T^{n-k-1} \cdot (0,1,1,1,2,1,1,2,2,1,1,2,2,3,3,1)\right] \cdot (0,0,0,1,0\dots,0,0) + \frac{n-k-1}{2}\,.
\end{aligned}$$

The matrix T is diagonalizable, with some complex sixth roots of unity among the eigenvalues. In fact, simplifying in SAGE we obtain

$$\mathbb{E}(\sigma(R_n)|E_k) = \alpha^{(4)}_{n-k} = \frac{n-k-1}{2} + \frac{13}{9} + a(n-k-1)\,, \tag{5.10}$$

where

$$a(m) := -\frac{1}{9\times 2^{m+1}}\left(9 + 6\sqrt{3}\sin\left(\frac{2}{3}\pi m\right) - 8\sqrt{3}\sin\left(\frac{1}{3}\pi m\right) + 5\cos(\pi m) - 6\cos\left(\frac{1}{3}\pi m\right)\right).$$

5.3.3.3. *Odd case:* $1 \le k < n$*,* k *odd.* Assume the event E_k, with odd $k < n$. Then the walker starts in state $A^{(16)}$ and walks for $n-k-1$ steps before taking four final steps to clear carries.

It follows that

$$\begin{aligned}
\mathbb{E}(\sigma(R_n)|E_k) &= \alpha^{(16)}_{n-k} \\
&= (T^{n-k-1}v_1 + (n-k-1)d) \cdot (0,0,\dots,0,1) \\
&= \left[T^{n-k-1} \cdot (0,1,1,1,2,1,1,2,2,1,1,2,2,3,3,1)\right] \cdot (0,0,\dots,0,1) + \frac{n-k-1}{2}\,.
\end{aligned}$$

Simplifying in SAGE, this becomes

$$\mathbb{E}(\sigma(R_n)|E_k) = \alpha^{(16)}_{n-k} = \frac{n-k-1}{2} + \frac{13}{9} + b(n-k-1), \tag{5.11}$$

where

$$b(m) := \frac{1}{27\times 2^{m+1}}\left(27 - 15\cos(\pi m) - 36\cos\left(\frac{1}{3}\pi m\right) - 48\sqrt{3}\sin\left(\frac{1}{3}\pi m\right)\right).$$

5.3.4. Total expectation. This section is dedicated to the proof of the following proposition, which, in view of Lemma 5.3.1, will complete the proof of Theorem 1.5.3.

PROPOSITION 5.3.1.

$$\mathbb{E}(\sigma(R_n)) = \frac{n+1}{2} - \frac{5}{9} + \frac{b_n}{9 \times 2^{n-1}}\,. \tag{5.12}$$

We will reduce the proof of the proposition to the evaluation of an auxiliary function A, which we define next and then evaluate as a lemma.

DEFINITION 5.3.6. With a and b as in (5.10) and (5.11), define the function $A : \mathbb{Z}^+ \to \mathbb{R}$ by

$$A(n) = \sum_{\substack{k=2 \\ k \text{ even}}}^{n-1} \left(a(n-k-1)\frac{1}{2^k} \right) + \sum_{\substack{k=1 \\ k \text{ odd}}}^{n-1} \left(b(n-k-1)\frac{1}{2^k} \right), \tag{5.13}$$

for $n > 2$, $A(1) = 0$, and $A(2) = -2/9$.

LEMMA 5.3.3. *For $n \geq 1$, we have*

$$A(n) = \frac{1+(-1)^n}{2^{n+1}} + \frac{\rho_n}{9 \times 2^{n+1}}\,,$$

where $(\rho_n)_{n=0}^{\infty} := \overline{(-10, 0, -34, -48, -58, 12)}$.

We will prove the lemma in the next section. If we assume its validity for now, then we can verify (5.12) as follows.

PROOF OF PROPOSITION 5.3.1. Recall the standard *total expectation formula* for $\mathbb{E}(\sigma(R_n))$:

$$\mathbb{E}(\sigma(R_n)) = \sum_{k=1}^{n+1} \mathbb{E}(\sigma(R_n)|E_k)P(E_k)\,.$$

If we substitute into the latter formula the values (5.8) for $P(E_k)$, as well as the values (5.9), (5.10), and (5.11) for $\mathbb{E}(\sigma(R_n)|E_k)$, then we obtain

$$
\begin{aligned}
\text{(5.14)} \qquad \mathbb{E}(\sigma(R_n)) &= \sum_{k=1}^{n+1} \mathbb{E}(\sigma(R_n)|E_k)P(E_k) \\
&= \frac{1}{2^{n-1}} + \sum_{\substack{k=2 \\ k \text{ even}}}^{n-1} \mathbb{E}(\sigma(R_n)|E_k)P(E_K) + \sum_{\substack{k=1 \\ k \text{ odd}}}^{n-1} \mathbb{E}(\sigma(R_n)|E_k)P(E_k) \\
&= \frac{1}{2^{n-1}} + \left(\frac{n-1}{2} + \frac{13}{9}\right)\left(\sum_{k=1}^{n-1} \frac{1}{2^k}\right) + \left(\sum_{k=1}^{n-1} \frac{-k}{2^{k+1}}\right) \\
&\quad + \sum_{\substack{k=2 \\ k \text{ even}}}^{n-1} \left(a(n-k-1)\frac{1}{2^k}\right) + \sum_{\substack{k=1 \\ k \text{ odd}}}^{n-1} \left(b(n-k-1)\frac{1}{2^k}\right) \\
&= \frac{1}{2^{n-1}} + \left(\frac{n-1}{2} + \frac{13}{9}\right)\left(1 - \frac{1}{2^{n-1}}\right) + \left(\frac{1}{2}\right)^n (n+1) - 1 + A(n) \\
&= \frac{5}{9 \times 2^{n-1}} + \left(\frac{n+1}{2} - \frac{5}{9}\right) + A(n)\,,
\end{aligned}
$$

where in the second to last inequality we have used the identities $\sum_{k=1}^{n-1} 2^{-k} = 1 - 2^{1-n}$ and

$$
\sum_{k=1}^{n-1} \frac{-k}{2^{k+1}} = \left(\frac{1}{2}\right)^n (n+1) - 1\,,
$$

and the last equality is just simplification. By Lemma 5.3.3, we can rewrite (5.14) as

$$
\begin{aligned}
\text{(5.15)} \qquad \mathbb{E}(\sigma(R_n)) &= \frac{5}{9 \times 2^{n-1}} + \left(\frac{n+1}{2} - \frac{5}{9}\right) + \frac{1+(-1)^n}{2^{n+1}} + \frac{\rho_n}{9 \times 2^{n+1}} \\
&= \frac{n+1}{2} - \frac{5}{9} + \frac{5 + (1+(-1)^n)(9/4) + (\rho_n/4)}{9 \times 2^{n-1}} \\
&= \frac{n+1}{2} - \frac{5}{9} + \frac{\rho'_n}{9 \times 2^{n-1}}\,,
\end{aligned}
$$

where

$$
\rho'_n := 5 + (1+(-1)^n)(9/4) + (\rho_n/4)\,,
$$

for $n \geq 0$. But it is easy to check that $\rho'_n = b_n$ for $n \geq 0$, so the proof of Proposition 5.3.1 is complete by virtue of (5.15). □

This completes the proof of Theorem 1.5.3, modulo the final task of verifying Lemma 5.3.3, which we do in the next section.

5.3.5. Proof of Lemma 5.3.3. We must evaluate the expression $A(n)$ from (5.13) and verify the identity in the lemma. For $n = 1$ or $n = 2$ this can be checked directly. For arbitrary $n \geq 3$, we start by making some simplifications. Specifically, observe from (5.10) and (5.11) that we may write

$$
\begin{aligned}
a(m) &= -\frac{1}{2^{m+1}} - \frac{1}{9 \times 2^{m+1}} \tilde{a}(m), \\
b(m) &= \frac{1}{2^{m+1}} + \frac{1}{27 \times 2^{m+1}} \tilde{b}(m)\,,
\end{aligned}
$$

where

$$
\begin{aligned}
\tilde{a}(m) &:= 6\sqrt{3}\sin(2\pi m/3) - 8\sqrt{3}\sin(\pi m/3) + 5\cos(\pi m) - 6\cos(\pi m/3)\,, \\
\tilde{b}(m) &:= -15\cos(\pi m) - 36\cos(\pi m/3) - 48\sqrt{3}\sin(\pi m/3)\,.
\end{aligned}
$$

With this notation, we can rewrite (5.13) as

$$
\begin{aligned}
A(n) &= \sum_{\substack{k=2 \\ k \text{ even}}}^{n-1} \left(a(n-k-1)\frac{1}{2^k} \right) + \sum_{\substack{k=1 \\ k \text{ odd}}}^{n-1} \left(b(n-k-1)\frac{1}{2^k} \right) \\
&= \sum_{\substack{k=2 \\ k \text{ even}}}^{n-1} \left(-\frac{1}{2^n} - \frac{1}{9 \times 2^n}\tilde{a}(n-m-1) \right) + \sum_{\substack{k=1 \\ k \text{ odd}}}^{n-1} \left(\frac{1}{2^n} + \frac{1}{27 \times 2^n}\tilde{b}(n-m-1) \right)\,.
\end{aligned}
$$

The latter identity can be rewritten, upon observing that

$$
-\frac{1}{2^n}\left(\sum_{\substack{k=2 \\ k \text{ even}}}^{n-1} 1 \right) + \frac{1}{2^n}\left(\sum_{\substack{k=1 \\ k \text{ odd}}}^{n-1} 1 \right) = \frac{1+(-1)^n}{2^{n+1}}\,,
$$

in the following way:

$$
A(n) = \frac{1+(-1)^n}{2^{n+1}} + \frac{-1}{9 \times 2^n}\left[\sum_{\substack{k=2 \\ k \text{ even}}}^{n-1} \tilde{a}(n-k-1) \right] + \frac{1}{27 \times 2^n}\left[\sum_{\substack{k=1 \\ k \text{ odd}}}^{n-1} \tilde{b}(n-k-1) \right]\,. \tag{5.16}
$$

The lemma's proof has been reduced then to the evaluation in (5.16) of the two summations

$$\tilde{A}(n) := \sum_{\substack{k=2 \\ k \text{ even}}}^{n-1} \tilde{a}(n-k-1)$$

and

$$\tilde{B}(n) := \sum_{\substack{k=1 \\ k \text{ odd}}}^{n-1} \tilde{b}(n-k-1)\,.$$

We will evaluate them separately and then show that

$$\frac{-1}{9 \times 2^n}\tilde{A}(n) + \frac{1}{27 \times 2^n}\tilde{B}(n) = \frac{\rho_n}{9 \times 2^{n-1}},$$

which, by (5.16), will imply the desired conclusion that

$$A(n) = \frac{1 + (-1)^n}{2^{n+1}} + \frac{\rho_n}{9 \times 2^{n-1}},$$

and thus complete the proof.

5.3.5.1. *Evaluation of $\tilde{A}(n)$.* Assume $n \geq 3$. To evaluate $\tilde{A}(n) = \sum_{\substack{k=2 \\ k \text{ even}}}^{n-1} \tilde{a}(n-k-1)$, we make the change of variable $m = n - k - 1$ and write

$$\tilde{A}(n) = \sum_{\substack{m=0 \\ n-m \text{ odd}}}^{n-3} \tilde{a}(m)\,. \tag{5.17}$$

Recall that $\tilde{a}(m)$ is the sum of four trigonometric terms. We can express these as periodic functions of m, as follows:

$$\begin{aligned}
\left(6\sqrt{3}\sin(2\pi m/3)\right)_{m=0}^{\infty} &= \overline{(0, 9, -9)} \\
\left(-8\sqrt{3}\sin(\pi m/3)\right)_{m=0}^{\infty} &= \overline{(0, -12, -12, 0, 12, 12)} \\
(5\cos(\pi m))_{m=0}^{\infty} &= \overline{(5, -5)} \\
(-6\cos(\pi m/3))_{m=0}^{\infty} &= \overline{(-6, -3, 3, 6, 3, -3)}
\end{aligned}$$

Summing these terms for each m, one finds that $(\tilde{a}(m))_{m=0}^{\infty} = \overline{(-1, -11, -13, 1, 29, -5)}\,.$

With these values of $\tilde{a}(m)$ it is straightforward case analysis to deduce evaluations of $\tilde{A}(n)$ in (5.17) that depend only on the congruence of n modulo 6. The result is the following table.

Congruence of n modulo 6	Value of $\tilde{A}(n) = \sum_{\substack{k=2 \\ k \text{ even}}}^{n-1} \tilde{\alpha}(n-k-1) = \sum_{\substack{m=0 \\ n-m \text{ odd}}}^{n-3} \tilde{\alpha}(m)$
0	$5 - 15\left(\frac{n}{6}\right)$
1	$15\left(\frac{n-1}{6}\right)$
2	$-15\left(\frac{n-2}{6}\right)$
3	$-1 + 15\left(\frac{n-3}{6}\right)$
4	$-11 - 15\left(\frac{n-4}{6}\right)$
5	$-14 + 15\left(\frac{n-5}{6}\right)$

This information can in turn be compressed into the following formula: For $n \geq 3$,

$$\sum_{\substack{k=2 \\ k \text{ even}}}^{n-1} \tilde{a}(n-k-1) = \frac{5n}{2}(-1)^{n+1} + \frac{1}{2}\alpha_n\,, \tag{5.18}$$

where

$$(\alpha_n)_{n=0}^{\infty} = \overline{(10, -5, 10, -17, -2, -53)}\,.$$

5.3.5.2. *Evaluation of* $\tilde{B}$. Assume $n \geq 3$. To evaluate $\tilde{B}(n) = \sum_{\substack{k=1 \\ k \text{ odd}}}^{n-1} \tilde{b}(n-k-1)$, we make the change of variable $m = n-k-1$ and write

$$\tilde{B}(n) = \sum_{\substack{m=0 \\ n-m \text{ even}}}^{n-2} \tilde{b}(m)\,. \tag{5.19}$$

Recall that $\tilde{b}(m)$ is the sum of three trigonometric terms. We can express these as periodic functions of m, as follows:

$$(15\cos(\pi m))_{m=0}^{\infty} = \overline{(-15, 15)}$$

$$(-36\cos(\pi m/3))_{m=0}^{\infty} = \overline{(-36, -18, 18, 36, 18, -18)}$$

$$\left(-48\sqrt{3}\sin(\pi m/3)\right)_{m=0}^{\infty} = \overline{(0, -72, -72, 0, 72, 72)}$$

Summing these terms for each m, one finds that

$$(\tilde{b}(m))_{m=0}^{\infty} = \overline{(-51, -75, -69, 51, 75, 69)}\,.$$

As we did with $\tilde{A}(n)$, we can evaluate $\tilde{B}(n)$ in (5.19) by considering congruence of n modulo 6. The result is the following table.

Congruence of n modulo 6	Value of $\tilde{B}(n) = \sum_{\substack{k=1\\ k \text{ odd}}}^{n-1} \tilde{b}(n-k-1) = \sum_{\substack{m=0\\ n-m \text{ even}}}^{n-2} \tilde{b}(m)$
0	$-45\left(\frac{n}{6}\right)$
1	$45\left(\frac{n-1}{6}\right)$
2	$-51 - 45\left(\frac{n-2}{6}\right)$
3	$-75 + 45\left(\frac{n-3}{6}\right)$
4	$-120 - 45\left(\frac{n-4}{6}\right)$
5	$-24 + 45\left(\frac{n-5}{6}\right)$

This information can be compressed into the following formula: For $n \geq 3$,

$$\sum_{\substack{k=1\\ k \text{ odd}}}^{n-1} \tilde{b}(n-k-1) = \frac{15n}{2}(-1)^{n+1} + \frac{1}{2}\beta_n\,, \tag{5.20}$$

where

$$(\beta_n)_{n=0}^{\infty} = \overline{(0, -15, -72, -195, -180, -123)} = 3 \times \overline{(0, -5, -24, -65, -60, -41)}\,.$$

5.3.5.3. *Evaluation of* $A(n)$*.* Recall from (5.16) that

$$A(n) = \frac{1 + (-1)^n}{2^{n+1}} + \frac{-1}{9 \times 2^n}\tilde{A}(n) + \frac{1}{27 \times 2^n}\tilde{B}(n)\,.$$

In view of (5.18) and (5.20), we have

$$\frac{-1}{9 \times 2^n}\tilde{A}(n) + \frac{1}{27 \times 2^n}\tilde{B}(n) = \frac{1}{9 \times 2^{n+1}}\left(-\alpha_n + \beta_n/3\right)\,.$$

Since $-\alpha_n + \beta_n/3 = \rho_n$, the proof of Lemma 5.3.3 is complete.

Bibliography

[And76] G. Andrews, *The Theory of Partitions*, Addison-Wesley Publishing Company, 1976.

[Bai35] W. Bailey, *Generalized Hypergeometric Series*, Cambridge University Press, 1935.

[BD15] C. Banderier and M. Drmota, *Formulae and asymptotics for coefficients of algebraic functions*, Combinatorics, Probability and Computing **24** (2015), 1–53.

[Bel61] R. Bellman, *A Brief Introduction to Theta Functions*, Holt, Rinehart and Winston, Inc, 1961.

[BTWZ19] A. Bostan, J. Tirrell, B. Westbury, and Y. Zhang, *On sequences associated to the invariant theory of rank two simple Lie algebras*, 2019, 1911.10288.

[Coh17] H. Cohn, *A conceptual breakthrough in sphere packing*, Not. Amer. Math. Soc. **64** (2017), 102–115.

[Dar78] J.-G. Darboux, *Mémoire sur l'approximation des fonctions de très grands nombres, et sur une classe étendu de d'eveloppements en série*, Journal de Math. Pures et Appliquées **3** (1878), no. 4, 5–56.

[DB58] N. De Bruijn, *Asymptotic Methods in Analysis*, North-Holland Publishing Company, 1958.

[DF04] D. Dummit and R. Foote, *Abstract Algebra (3rd ed.)*, John Wiley and Sons, Inc., 2004.

[DG08] B. Datskovsky and P. Guerzhoy, *P-adic interpolation of Taylor coefficients of modular forms*, Math. Ann. **340** (2008), no. 2, 465–476.

[Drm04] M. Drmota, *Combinatorics and asymptotics on trees*, CUBO, A Mathematical Journal **6** (2004), no. 2, 105–136.

[DS16] F. Diamond and J. Shurman, *A First Course in Modular Forms*, Springer, 2016.

[Fek23] M. Fekete, *Über die verteilung der wurzeln bei gewissen algebraischen gleichungen mit ganzzahligen koeffizienten*, Mathematische Zeitschrift **17** (1923), no. 1, 228–249.

[Fin78] H. Finkelstein, *Solving equations in groups: a survey of Frobenius' theorem*, Periodica Mathematica Hungarica **9** (1978), no. 3, 187–476.

[FO90] P. Flajolet and A. Odlzyko, *Singularity analysis of generating functions*, SIAM J. Discrete Math. **3** (1990), no. 2, 216–240.

[FS09] P. Flajolet and R. Sedgewick, *Analytic Combinatorics*, Cambridge University Press, 2009.

[GM93] D. Grabiner and P. Magyar, *Random walks in Weyl chambers and the decomposition of tensor powers*, Journal of Algebraic Combinatorics **2** (1993), 216–240.

[GMR20] P. Guerzhoy, M. Mertens, and L. Rolen, *Periodicities for Taylor coefficients of half-integral weight modular forms*, Pacific J. of Math **307** (2020), 137–157.

[GZ92] I. Gessel and D. Zeilberger, *Random walks in a Weyl chamber*, Proc. Amer. Math. Soc. **115** (1992), no. 1, 27–31.

[Hil59] E. Hille, *Analytic Function Theory, vol. 1*, Ginn and Company, 1959.

[Hum72] J. Humphreys, *Introduction to Lie Algebras and Representation Theory*, Springer, 1972.

[KL03] I. Krasikov and J. Lagarias, *Bounds for the $3x+1$ problem using difference inequalities*, Acta Arith **109** (2003), no. 3, 237–258.

[Kob93] N. Koblitz, *Introduction to Elliptic Curves and Modular Forms, 2nd ed.*, Springer, 1993.

[Kup94] G. Kuperberg, *The quantum G_2 link invariant*, Internat. J. Math. **5** (1994), no. 1, 61–85.

[Kup96] ———, *Spiders for rank 2 Lie algebras*, Comm. Math. Phys. **180** (1996), no. 1, 109–151.

[Lag85] J. Lagarias, *The $3x+1$ problem and its generalizations*, The American Mathematical Monthly **92** (1985), 3–23.

[Lag10] *The Ultimate Challenge: The $3x+1$ Problem*, (J. Lagarias, ed.), American Math. Society, 2010.

[Lan02] S. Lang, *Algebra (3rd ed.)*, Springer Science + Business Media LLC, 2002.

[Leg08] A. Legendre, *Essai sur la théorie des nombres (2nd ed.)*, Paris, Chez Courcier, Imprimeur - Libraire pour les Mathématiques, quai des Augustins, no 57, 1808.

[LS14] H. Larson and G. Smith, *Congruence properties of Taylor coefficients of modular forms*, Int. J. Number Theory **10** (2014), 1504–1518.

[Mat10] K. Matthews, *Generalized $3x+1$ mappings: Markov chains and ergodic theory*, In: The Ultimate Challenge: The $3x+1$ Problem (J. Lagarias, ed.), American Math. Society, 2010, pp. 79–103.

[MM78] A. Meir and J. Moon, *On the altitude of nodes in random trees*, Can. J. Math **30** (1978), no. 5, 997–1015.

[MM89] A. Meir and J. Moon, *On an asymptotic method in enumeration*, J. of Combinatorial Number Theory, Series A **51** (1989), no. 1, 77–89.

[Pol37] G. Polya, *Pólya, george. kombinatorische anzahlbestimmungen für gruppen, graphen und chemische verbindungen.*, Acta Math. **68** (1937), 145–254.

[Rom20] D. Romik, *The Taylor coefficients of the Jacobi theta constant θ_3*, Ramanujan Journal **52** (2020), 275–290.

[RS] D. Romik and R. Scherer, *Identities for average values of iterates of the Syracuse map*, in preparation.

[RS20] ———, *Alternative summation orders for the Eisenstein series G_2 and Weierstrass $\wp$-function*, Rocky Mountain J. Math **50** (2020), no. 4, 1473–1482.

[Sch20] R. Scherer, *A criterion for sharpness in tree enumeration and the asymptotic number of triangulations in Kuperberg's G_2 spider*, 2020, https://arxiv.org/pdf/2003.07984.pdf.

[Sch21] ———, *Congruences modulo primes of the Romik sequence related to the Taylor expansion of the Jacobi theta constant θ_3*, Ramanujan Journal **54** (2021), 427–448.

[Shi73] G. Shimura, *On modular forms of half integral weight*, Annals of Math. **97** (1973), no. 3, 440–481.

[SI20] N. J. A. Sloane and T. O. F. Inc., *The On-line Encyclopedia of Integer Sequences*, online source, accessed April 2020, http://oeis.org.

[Smi59] K. Smith, *Analytic Function Theory, vol. 1*, Ginn and Company, 1959.

[SS03] E. Stein and R. Shakarchi, *Complex Analysis (Princeton Lectures in Analysis, no. 2)*, Princeton University Press, 2003.

[Sta99] R. Stanley, *Enumerative Combinatorics, vol. 2*, Cambridge University Press, 1999.

[Tao20] T. Tao, *Almost all orbits of the Collatz map attain almost bounded values*, 2020, 1909.03562v3.

[TZ04] T. Tate and S. Zeldtich, *Lattice path combinatorics and asymptotics of multiplicities of weights in tensor powers*, Journal of Functional Analysis **217** (2004), no. 2, 402–447.

[VD93] F. Villegas and Z. D, *Square roots of central values of Hecke L-series*, In: Advances in Number Theory (F. Gouvea and N. Yui, eds.), Clarendon Press, 1993, pp. 81–99.

[Via17] M. Viazovska, *The sphere packing problem in dimension 8.*, Ann. Math **185** (2017), 991–1015.

[Wak20] T. Wakhare, *Romik's conjecture for the Jacobi theta function*, J. of Number Theory **215** (2020), no. 2, 275–296.

[Wes07] B. Westbury, *Enumeration of non-positive planar trivalent graphs*, Journal of Algebraic Combinatorics **25** (2007), no. 4, 357–373.

[Wol20] *Wolfram Research*, online source, accessed Oct. 2020, https://functions.wolfram.com/Hypergeometric Functions/Hypergeometric2F1/06/01/04/01/02.

[Woo86] D. Wood, *Theory of Computaiton*, Wiley, 1986.

[Zag89] D. Zagier, *Introduction to Modular Forms*, In: From Number Theory to Physics (M. Waldschmidt, P. Moussa, J.-M. Luck, and C. Itzykosn, eds.), Springer-Verlag, 1989, pp. 238–291.

[Zag08] ______, *Elliptic Modular Forms and Their Applications*, In: The 1-2-3 of modular forms (K. Ranestad, ed.), Springer, 2008, pp. 1–103.