A method for determining the mod-2^k behaviour of recursive sequences, with applications to subgroup counting

M. Kauers*

Research Institute for Symbolic Computation
Johannes Kepler Universität, Altenbergerstraße 69
A-4040 Linz, Austria

WWW: http://www.kauers.de/

C. Krattenthaler†

Fakultät für Mathematik, Universität Wien
Nordbergstraße 15, A-1090 Vienna, Austria

WWW: http://www.mat.univie.ac.at/~kratt

T. W. Müller‡

School of Mathematical Sciences, Queen Mary
& Westfield College, University of London,
Mile End Road, London E1 4NS, United Kingdom.

Submitted: May 3, 2011; Accepted: Jun 9, 2012; Published: Jun 20, 2012
2010 Mathematics Subject Classifications: Primary 20E06; Secondary 05A15 05E99 11A07 20E07 33F10 68W30

Dedicated to Doron Zeilberger

Abstract

We present a method to obtain congruences modulo powers of 2 for sequences given by recurrences of finite depth with polynomial coefficients. We apply this method to Catalan numbers, Fuß–Catalan numbers, and to subgroup counting functions associated with Hecke groups and their lifts. This leads to numerous new results, including many extensions of known results to higher powers of 2.

*Research supported by the Austrian Science Foundation FWF, grant Y464-N18.

†Research partially supported by the Austrian Science Foundation FWF, grants Z130-N13 and S9607-N13, the latter in the framework of the National Research Network "Analytic Combinatorics and Probabilistic Number Theory".

‡Research supported by Lise Meitner Grant M1201-N13 of the Austrian Science Foundation FWF.

1 Introduction

Ever since the work of Sylow [35], Frobenius [12, 13], and P. Hall [17], the study of congruences for subgroup numbers and related numerical quantities of groups has played an important role in group theory.

Divisibility properties of subgroup numbers of (finitely generated) infinite groups may to some extent be viewed as some kind of analogue to these classical results for finite groups. To the best of our knowledge, the first significant result in this direction was obtained by Stothers [34]: *the number of index-n-subgroups in the inhomogeneous modular group $PSL_2(\mathbb{Z})$ is odd if, and only if, n is of the form 2^k-3 or $2^{k+1}-6$, for some positive integer $k \geq 2$.* A different proof of this result was given by Godsil, Imrich, and Razen [14].

The systematic study of divisibility properties of subgroup counting functions for infinite groups begins with [27]. There, the parity of subgroup numbers and the number of free subgroups of given finite index are determined for arbitrary Hecke groups $\mathfrak{H}(q) = C_2 * C_q$ with $q \geq 3$. Subsequently, the results of [27] were generalised to larger classes of groups and arbitrary prime modulus in [3, 20, 25, 26, 28]. A first attempt at obtaining congruences modulo higher prime powers was made in [29], where the behaviour of subgroup numbers in $PSL_2(\mathbb{Z}) \cong \mathfrak{H}(3)$ is investigated modulo 8 and a congruence modulo 16 is derived for the number of free subgroups of given index in $PSL_2(\mathbb{Z})$.

A common feature of all the above listed sequences of subgroup numbers is that they obey recurrences of finite depth with polynomial coefficients. The purpose of this paper is to present a new method for determining congruences modulo arbitrarily large powers of 2 for sequences described by such recurrences. Our method is inspired by the observation that many of the aforementioned results say in essence that the generating function for the subgroup numbers under consideration, when reduced modulo a 2-power, can be expressed as a polynomial in the basic series

$$\Phi(z) = \sum_{n \geq 0} z^{2^n} \tag{1.1}$$

with coefficients that are Laurent polynomials in z. What our method affords is an algorithmic procedure to find such polynomial expressions, provided they exist. By applying our method to Catalan numbers, to (certain) Fuß–Catalan numbers, and to various subgroup counting problems in Hecke groups and their lifts, we obtain far-reaching generalisations and extensions of the previously mentioned results. In order to give a concrete illustration, the recent result [22, Theorems 6.1–6.6] of Liu and Yeh determining the

behaviour of Catalan numbers Cat_n modulo 64 can be compactly written in the form

$$\sum_{n=0}^{\infty} \mathrm{Cat}_n\, z^n = 32z^5 + 16z^4 + 6z^2 + 13z + 1 + \left(32z^4 + 32z^3 + 20z^2 + 44z + 40\right)\Phi(z)$$
$$+ \left(16z^3 + 56z^2 + 30z + 52 + \frac{12}{z}\right)\Phi^2(z) + \left(32z^3 + 60z + 60 + \frac{28}{z}\right)\Phi^3(z)$$
$$+ \left(32z^3 + 16z^2 + 48z + 18 + \frac{35}{z}\right)\Phi^4(z) + \left(32z^2 + 44\right)\Phi^5(z)$$
$$+ \left(48z + 8 + \frac{50}{z}\right)\Phi^6(z) + \left(32z + 32 + \frac{4}{z}\right)\Phi^7(z) \qquad \text{modulo } 64, \quad (1.2)$$

as may be seen by a straightforward (but rather tedious) computation. Our method can not only *find* this result, but it produces as well corresponding formulae modulo *any* given power of 2 in a completely automatic fashion, see Theorems 13 and 14 in Section 5.

In a sense, which is made precise in Section 4, our method is very much in the spirit of Doron Zeilberger's philosophy that *mathematicians should train computers to automatically produce theorems*. Indeed, Theorems 13, 19, 21, 33, 36 imply that our algorithm is able to produce a theorem on the behaviour modulo *any* given 2-power of the subgroup counting functions featuring in these theorems, and, if fed with a concrete 2-power, our implementation will diligently output the corresponding result (provided the input does not cause the available computer resources to be exceeded ...). Moreover, when discussing subgroup numbers of lifts of $PSL_2(\mathbb{Z})$, (such as the homogeneous modular group $SL_2(\mathbb{Z})$), a crucial role is also played by an application of the holonomic functions approach to finding recurrences for multi-variate hypergeometric sums, pioneered by Wilf and Zeilberger [37, 39], and further developed in [4, 5, 19].

The rest of this introduction is devoted to a more detailed description of the contents of this paper. In Section 2 we discuss our main character, the formal power series $\Phi(z)$ defined in (1.1). While $\Phi(z)$ is transcendental over $\mathbb{Q}[z]$ (or, equivalently, over $\mathbb{Z}[z]$), it is easy to see that it is algebraic modulo powers of 2. The focus in that section is on polynomial identities for $\Phi(z)$ modulo a given 2-power which are of *minimal degree*. Then, in Section 4, we describe our method of expressing the generating function of a recursive sequence, when reduced modulo a given 2-power, as a polynomial in $\Phi(z)$ with coefficients that are Laurent polynomials in z. The method relies in an essential way on the polynomial identities from Section 2. The problem how to extract the explicit value of a concrete coefficient in a polynomial expression in $\Phi(z)$ (such as (1.2)) modulo a given 2-power is discussed in Section 3, where we present an efficient algorithm performing this task. This algorithm is of theoretical value (minimal length relations between powers of $\Phi(z)$ such as the ones in Proposition 2 are established by applying this algorithm to the powers of $\Phi(z)$; see also Appendix A) as well as of practical significance, as is demonstrated by the derivations of Theorems 27 and 31.

As a first illustration of our method, we apply it to Catalan numbers, thereby significantly improving numerous earlier results in the literature; see Section 5. This is contrasted in Section 6 with an example (concerning particular Fuß–Catalan numbers)

where our method is bound to fail. The reason is spelled out in Theorem 15, which, at the same time, also gives a new description for the parity pattern of the numbers of free subgroups of given index in the Hecke group $\mathfrak{H}(7)$.

The subsequent sections contain several applications of our method to the problem of determining congruences modulo a given 2-power for numbers of subgroups of Hecke groups $\mathfrak{H}(q)$ and their lifts

$$\Gamma_m(q) = C_{2m} \underset{C_m}{*} C_{qm} = \left\langle x, y \,\middle|\, x^{2m} = y^{qm} = 1,\, x^2 = y^q \right\rangle, \quad m \geq 1. \tag{1.3}$$

Ubiquitous in these applications is — explicitly or implicitly — the intimate relation between subgroup numbers of a group Γ and numbers of permutation representations of Γ, in the form of identities between the corresponding generating functions. This is directly visible in the folklore result (11.1) (which is not only used in Sections 11, 12, and 14, but also lies behind the crucial differential equation (9.1) in Section 9; cf. its derivation in [14]), and also indirectly in Lemma 17 via the A-invariants $A_\mu(\mathfrak{H}(q))$, see [27, Sec. 2.2]. In the cases relevant here, the numbers of permutation representations of Γ satisfy linear recurrences with polynomial coefficients — to make these explicit may require the algorithmic machinery around the "holonomic paradigm" (cf. [4, 5, 19, 23, 31, 37, 39]), see Sections 11 and 12 for corresponding examples. Via the aforementioned generating function relation, such a recurrence can be translated into a Riccati-type differential equation for the generating function of the subgroup numbers that we are interested in. It is here, where our method comes in: it is tailor-made for being applied to formal power series $F(z)$ satisfying this type of differential equation, and it affords an algorithmic procedure to find a polynomial in $\Phi(z)$ which agrees, after reduction of the coefficients of $F(z)$ modulo a given power of 2, with the power series $F(z)$.

We start in Section 7 with free subgroup numbers of lifts $\Gamma_m(q)$, for primes $q \geq 3$, where we prepare the ground for application of our method. More specifically, in Proposition 18 we present a lower bound for the 2-adic valuation of the number of free subgroups of index n in $\Gamma_m(q)$, where q is a Fermat prime. In particular, this result implies that the sequence of free subgroup numbers under consideration is essentially zero modulo a given 2-power in the case when m is even. In Section 8, we show that our method provides an algorithm for determining these numbers of free subgroups of $\Gamma_m(3)$ modulo any given 2-power in the case when m is odd. The corresponding results (see Theorems 19 and 20) go far beyond the previous result [29, Theorem 1] on the behaviour of the number of free subgroups of $PSL_2(\mathbb{Z})$ modulo 16. Our method provides as well an algorithm for determining the number of *all* subgroups of index n in $PSL_2(\mathbb{Z})$ modulo powers of 2, as we demonstrate in Section 9. Not only are we able to provide a new proof of Stothers' result [34] (which was stated in the second paragraph above), but our method leads as well to refinements modulo arbitrary powers of 2 of Stothers' result and of the mod-8 results in [29, Theorem 2] mentioned earlier; see Theorems 21 and 24. For the homogeneous modular group $SL_2(\mathbb{Z})$ (being isomorphic to the lift $\Gamma_2(3)$) and for the lift $\Gamma_3(3)$, however, our method from Section 4 fails already for the modulus $8 = 2^3$. We overcome this obstacle by instead tuning our computations with the target of obtaining results modulo $16 = 2^4$. Indeed, this leads to the determination of the number of subgroups of index n in $SL_2(\mathbb{Z})$

and in $\Gamma_3(3)$ modulo 8 (see Theorems 26 and 30), but direct application of our method does not produce corresponding results modulo 16. Only by an *enhancement* of the method, which we outline in Appendix D, we are able to produce descriptions of the subgroup numbers of $SL_2(\mathbb{Z})$ modulo 16, see Theorem 28. For the subgroup numbers of $\Gamma_3(3)$ even this enhancement fails, and this shows that the generating function for these subgroup numbers, when coefficients are reduced modulo 16, *cannot* be represented as a polynomial in $\Phi(z)$ with coefficients that are Laurent polynomials in z. Still, the results in Theorems 26, 28, and 30 go significantly beyond the earlier parity results [20, Eq. (6.3) with $|H| = 1$] for these groups. This is explained in Sections 11 and 12, with Section 10 preparing the ground by providing formulae for the number of permutation representations of $SL_2(\mathbb{Z})$ as well as other lifts of $PSL_2(\mathbb{Z})$. A further example where our method works for any 2-power is the subject of Section 13: there we apply the method to a functional equation (see (13.1)) extending the functional equation for Catalan numbers (producing *Fuß–Catalan numbers*), and show that it works for any given 2-power; see Theorem 33. In fact, we apply a variation of the method here, in that the basic series $\Phi(z)$ gets replaced by a slightly different series, which we denote by $\Phi_h(z)$ (see (13.3)). If Theorem 33 is combined with results from [27], then it turns out that our method provides as well an algorithm for determining the number of free subgroups of index n in a Hecke group $\mathfrak{H}(q)$ and its lifts, where q is a Fermat prime, modulo any given 2-power; see Corollary 34. The same assertion holds as well for the problem of determining the number of subgroups of index n in the Hecke group $\mathfrak{H}(5)$, again modulo any given 2-power (see Theorems 36 and 37 in Section 14). We conjecture that the same is true for Hecke groups $\mathfrak{H}(q)$, with q a Fermat prime (see Conjecture 38). The results of Sections 13 and 14 discussed above largely generalise the parity results [27, Cor. A', respectively Theorem B] for subgroup numbers of Hecke groups, although our results are not independent, in the sense that we base our analyses on prior results from [27].

Concluding the introduction, we remark that there is no principal obstacle to generalising our method to other basic series and moduli. For example, one may think of analysing the behaviour of recursive sequences modulo powers of any prime p in terms of the obvious generalisation of $\Phi(z)$, i.e., the series $\sum_{n\geq 0} z^{p^n}$. It is in fact not difficult to see that our results from Sections 5 and 13 for Fuß–Catalan numbers characterised by the functional equation (13.1) for their generating function have rather straightforward analogues for Fuß–Catalan numbers whose generating function satisfies the functional equation

$$z f^{p^h}(z) - f(z) + 1 = 0. \tag{1.4}$$

However we are not aware of any applications of this (or of variants) to congruence properties of subgroup numbers modulo powers of primes p different from 2. In fact, the known results (cf. [28] or [29, Theorem 3]) strongly point to the fact that the phenomena that appear modulo primes different from 2 cannot be captured by series of the type $\sum_{n\geq 0} z^{p^n}$. So, currently, we do not know of interesting applications in this direction, but we hope to be able to return to this circle of ideas in future publications.

Note. This paper is accompanied by several *Mathematica* files and a *Mathematica* note-

book so that an interested reader is able to redo (most of) the computations that are presented in this article. Files and notebook are available at the article's website `http://www.mat.univie.ac.at/~kratt/artikel/modlifts.html`.

2 The 2-power series $\Phi(z)$

Here we consider the formal power series $\Phi(z)$ defined in (1.1). This series is the principal character in the method for determining congruences of recursive sequences modulo 2-powers, which we describe in Section 4. It is well known that this series is transcendental over $\mathbb{Z}[z]$ (this follows for instance from the density argument used in the proof of Lemma 1 below). However, if the coefficients of $\Phi(z)$ are considered modulo a 2-power 2^γ, then $\Phi(z)$ obeys a polynomial relation with coefficients that are polynomials in z. The focus of this section is on what may be said concerning such polynomial relations, and, in particular, about those of minimal length.

Here and in the sequel, given power series (or Laurent series) $f(z)$ and $g(z)$, we write

$$f(z) = g(z) \text{ modulo } 2^\gamma$$

to mean that the coefficients of z^i in $f(z)$ and $g(z)$ agree modulo 2^γ for all i.

We say that a polynomial $A(z,t)$ in z and t is *minimal for the modulus* 2^γ, if it is monic (as a polynomial in t), has integral coefficients, satisfies $A(z,\Phi(z)) = 0$ modulo 2^γ, and there is no monic polynomial $B(z,t)$ with integral coefficients of t-degree less than that of $A(z,t)$ with $B(z,\Phi(z)) = 0$ modulo 2^γ. (Minimal polynomials are not unique; see Remark 3.) Furthermore, we let $v_2(\alpha)$ denote the 2-adic valuation of the integer α, that is, the maximal exponent e such that 2^e divides α.

The lemma below provides a lower bound for the degree of a polynomial that is minimal for the modulus 2^γ.

Lemma 1. *If $A(z,t)$ is minimal for the modulus 2^γ, then the degree d of $A(z,t)$ in t satisfies $v_2(d!) \geq \gamma$. In particular, the series $\Phi(z)$ is transcendental over $\mathbb{Z}[z]$.*

Proof. We introduce the following *density function* with respect to a given modulus 2^γ for a power series $f(z)$ in z:

$$D(f, 2^\gamma; n) := \big|\{e : 2^{n-1} \leq e < 2^n \text{ and } \langle z^e\rangle\, f(z) \not\equiv 0 \text{ modulo } 2^\gamma\}\big|, \qquad n = 1, 2, \ldots, \tag{2.1}$$

where $\langle z^e\rangle\, f(z)$ denotes the coefficient of z^e in $f(z)$. Setting

$$E_m(z) := \sum_{n_1 > \cdots > n_m \geq 0} z^{2^{n_1} + 2^{n_2} + \cdots + 2^{n_m}}, \tag{2.2}$$

simple counting yields that

$$D(E_m, 2^\gamma; n) = \binom{n-1}{m-1} \sim \frac{1}{(m-1)!} n^{m-1}, \qquad \text{as } n \to \infty. \tag{2.3}$$

(The modulus 2^γ does not play a role here.) Furthermore, by considering the binary representations of possible exponents e such that the coefficient of z^e in $\Phi^m(z)$ does not vanish, we have

$$D(\Phi^m, 2^\gamma; n) = \mathcal{O}\left(n^{m-1}\right), \qquad \text{as } n \to \infty. \tag{2.4}$$

Indeed, by direct expansion, we see that

$$\Phi^m(z) = m!\, E_m(z) + R_m(z), \tag{2.5}$$

where all monomials z^e which appear with non-vanishing coefficient in $R_m(z)$ have a binary expansion with at most $m-1$ digits 1. Consequently, again by elementary counting, we have

$$D(R_m, 2^\gamma; n) \le \binom{n-1}{m-2} + \binom{n-1}{m-3} + \cdots + \binom{n-1}{0},$$

and hence $D(R_m, 2^\gamma; n) = \mathcal{O}(n^{m-2})$ as $n \to \infty$.

Let us, by way of contradiction, suppose that the degree d of $A(z,t)$ satisfies $v_2(d!) < \gamma$. Considering (2.5) with $m = d$, we see that $E_d(z)$ appears in $\Phi^d(z)$ with a non-zero coefficient modulo 2^γ. Furthermore, the other terms in $\Phi^d(z)$ (denoted by $R_d(z)$ in (2.5)) have a density function modulo 2^γ which is asymptotically strictly smaller than the density function of $E_d(z)$. Consequently, if we remember (2.3), we have

$$D(\Phi^d, 2^\gamma; n) \sim \frac{d!}{(d-1)!} n^{d-1} = d n^{d-1}, \qquad \text{as } n \to \infty.$$

Moreover, by (2.4), all powers $\Phi^m(z)$ with $m < d$ have a density function modulo 2^γ which is asymptotically strictly smaller than n^{d-1}. Altogether, it is impossible that a linear combination of powers $\Phi^m(d)$, $m = 0, 1, \ldots, d$, with coefficients that are polynomials in z sums up to zero modulo 2^γ, a contradiction to our assumption that d is the degree of a minimal polynomial $A(z,t)$. The particular statement is an immediate consequence of the inequality just proven. □

Proposition 2. *Minimal polynomials for the moduli* $2, 4, 8, 16, 32, 64, 128$ *are*

$$\begin{aligned}
&t^2 + t + z && \text{modulo } 2,\\
&(t^2 + t + z)^2 && \text{modulo } 4,\\
&t^4 + 6t^3 + (2z+3)t^2 + (2z+6)t + 2z + 5z^2 && \text{modulo } 8,\\
&(t^2 + t + z)(t^4 + 6t^3 + (2z+3)t^2 + (2z+6)t + 2z + 5z^2) && \text{modulo } 16,\\
&(t^4 + 6t^3 + (2z+3)t^2 + (2z+6)t + 2z + 5z^2)^2 && \text{modulo } 32,\\
&(t^4 + 6t^3 + (2z+3)t^2 + (2z+6)t + 2z + 5z^2)^2 && \text{modulo } 64,\\
&t^8 + 124t^7 + t^6(68z+18) + t^5(124z+24) + t^4\left(62z^2 + 64z + 81\right)\\
&\quad + t^3\left(20z^2 + 76z + 28\right) + t^2\left(116z^3 + 114z^2 + 12z + 92\right)\\
&\quad + t\left(116z^3 + 28z^2 + 8z + 16\right) + 9z^4 + 124z^3 + 12z^2 + 112z && \text{modulo } 128.
\end{aligned}$$

Proof. In order to be consistent with Section 3, let us change notation and write

$$H_{1,1,\ldots,1}(z) := \sum_{n_1>\cdots>n_m\geq 0} z^{2^{n_1}+2^{n_2}+\cdots+2^{n_m}}$$

(with m occurrences of 1 in $H_{1,1,\ldots,1}(z)$). Note that the above series is identical with the series which we earlier denoted by $E_m(z)$. Straightforward calculations yield that

$$\Phi^2(z) = \Phi(z) + 2H_{1,1}(z) - z, \tag{2.6}$$

$$\Phi^3(z) = -2\sum_{n\geq 0} z^{3\cdot 2^n} + 3(1-z)\Phi(z) + 6H_{1,1}(z) + 6H_{1,1,1}(z) - 3z, \tag{2.7}$$

$$\begin{aligned}\Phi^4(z) = -12\sum_{n\geq 0} z^{3\cdot 2^n} - 8\sum_{n_1>n_2\geq 0} z^{3\cdot 2^{n_1}+2^{n_2}} - 8\sum_{n_1>n_2\geq 0} z^{2^{n_1}+3\cdot 2^{n_2}} + (13-18z)\Phi(z)\\ + (30-12z)H_{1,1}(z) + 36H_{1,1,1}(z) + 24H_{1,1,1,1}(z) + 5z^2 - 13z.\end{aligned} \tag{2.8}$$

In particular, relation (2.6), together with Lemma 1, immediately implies the claims about minimal polynomials for the moduli 2 and 4. Moreover, a simple computation using (2.6)–(2.8) shows that

$$\Phi^4(z) + 6\Phi^3(z) + (2z+3)\Phi^2(z) + (2z+6)\Phi(z) + 2z + 5z^2 = 0 \quad \text{modulo } 8. \tag{2.9}$$

Together with Lemma 1, this establishes the claims about minimal polynomials for the moduli 8, 16, 32, and 64. In order to prove the claim for the modulus 128, one uses the expressions for $\Phi^i(z)$, $i = 2, 3, \ldots, 8$, given above and in Appendix A. □

Remark 3. Minimal polynomials are highly non-unique: for example, the polynomial

$$(t^2+t+z)^2 + 2(t^2+t+z)$$

is obviously also a minimal polynomial for the modulus 4.

Based on the observations in Proposition 2 and Lemma 1, we propose the following conjecture.

Conjecture 4. *The degree of a minimal polynomial for the modulus 2^γ, $\gamma \geq 1$, is the least d such that $v_2(d!) \geq \gamma$.*

Remark 5. (1) Given the binary expansion of d, say

$$d = d_0 + d_1\cdot 2 + d_2\cdot 4 + \cdots + d_r\cdot 2^r, \quad 0\leq \gamma_i \leq 1,$$

by the well-known formula of Legendre [21, p. 10], we have

$$\begin{aligned} v_2(d!) &= \sum_{\ell=1}^{\infty}\left\lfloor \frac{d}{2^\ell}\right\rfloor = \sum_{\ell=1}^{\infty}\left\lfloor \sum_{i=0}^{r} d_i 2^{i-\ell}\right\rfloor = \sum_{\ell=1}^{\infty}\sum_{i=\ell}^{r} d_i 2^{i-\ell}\\ &= \sum_{i=1}^{r}\sum_{\ell=1}^{i} d_i 2^{i-\ell} = \sum_{i=1}^{r} d_i\left(2^i-1\right) = d - s(d), \end{aligned} \tag{2.10}$$

where $s(d)$ denotes the sum of digits of d in its binary expansion. Consequently, an equivalent way of phrasing Conjecture 4 is to say that the degree of a minimal polynomial for the modulus 2^γ is the least d with $d - s(d) \geq \gamma$.

(2) We claim that, in order to establish Conjecture 4, it suffices to prove the conjecture for $\gamma = 2^\delta - 1$, $\delta = 1, 2, \ldots$. If we take into account Lemma 1 plus the above remark, this means that it is sufficient to prove that, for each $\delta \geq 1$, there is a polynomial $A_\delta(z,t)$ of degree 2^δ such that

$$A_\delta(z, \Phi(z)) = 0 \quad \text{modulo } 2^{2^\delta - 1}. \tag{2.11}$$

For, arguing by induction, let us suppose that we have already constructed $A_1(z,t)$, $A_2(z,t), \ldots, A_m(z,t)$ satisfying (2.11). Let

$$\alpha = \alpha_1 \cdot 2 + \alpha_2 \cdot 4 + \cdots + \alpha_m \cdot 2^m, \quad 0 \leq \alpha_i \leq 1,$$

be the binary expansion of the even positive integer α. In this situation, we have

$$\prod_{\delta=1}^{m} A_\delta^{\alpha_\delta}(z, \Phi(z)) = 0 \quad \text{modulo } \prod_{\delta=1}^{m} 2^{\alpha_\delta(2^\delta - 1)} = \prod_{\delta=0}^{m} 2^{\alpha_\delta(2^\delta - 1)} = 2^{\alpha - s(\alpha)}. \tag{2.12}$$

On the other hand, the degree of the left-hand side of (2.12) as a polynomial in $\Phi(z)$ is $\sum_{\delta=1}^{m} \alpha_\delta 2^\delta = \alpha$.

Let us put these observations together. In view of (2.10), Lemma 1 says that the degree of a minimal polynomial for the modulus 2^γ cannot be smaller than the least integer, $d^{(\gamma)}$ say, for which $d^{(\gamma)} - s(d^{(\gamma)}) \geq \gamma$. (We remark that $d^{(\gamma)}$ must be automatically even.) If we take into account that the quantity $\alpha - s(\alpha)$, as a function in α, is weakly monotone increasing in α, then (2.12) tells us that, as long as $d^{(\gamma)} \leq 2 + 4 + \cdots + 2^m = 2^{m+1} - 2$, we have found a monic polynomial of degree $d^{(\gamma)}$, $B_\gamma(z,t)$ say, for which $B_\gamma(z, \Phi(z)) = 0$ modulo 2^γ, namely the left-hand side of (2.12) with α replaced by $d^{(\gamma)}$, to wit

$$B_\gamma(z,t) = \prod_{\delta=1}^{m} A_\delta^{d_\delta^{(\gamma)}}(z,t),$$

where $d^{(\gamma)} = d_1^{(\gamma)} \cdot 2 + d_2^{(\gamma)} \cdot 4 + \cdots + d_m^{(\gamma)} \cdot 2^m$ is the binary expansion of $d^{(\gamma)}$. Hence, it must necessarily be a minimal polynomial for the modulus 2^γ.

Since $(2^{m+1} - 2) - s(2^{m+1} - 2) = 2^{m+1} - 2 - m$, we have thus found minimal polynomials for all moduli 2^γ with $\gamma \leq 2^{m+1} - m - 2$. Now we should note that the quantity $\alpha - s(\alpha)$ makes a jump from $2^{m+1} - m - 2$ to $2^{m+1} - 1$ when we move from $\alpha = 2^{m+1} - 2$ to $\alpha = 2^{m+1}$ (the reader should recall that it suffices to consider even α). If we take $A_m^2(z,t)$, which has degree $2 \cdot 2^m = 2^{m+1}$, then, by (2.11), we also have a minimal polynomial for the modulus $\left(2^{2^m - 1}\right)^2 = 2^{2^{m+1} - 2}$ and, in view of the preceding remark, as well for all moduli 2^γ with γ between $2^{m+1} - m - 1$ and $2^{m+1} - 2$.

So, indeed, the first modulus for which we do not have a minimal polynomial is the modulus $2^{2^{m+1} - 1}$. This is the role which $A_{m+1}(z,t)$ (see (2.11) with $m+1$ in place of δ) would have to play.

The arguments above show at the same time that, supposing that we have already constructed $A_1(z,t), A_2(z,t), \ldots, A_m(z,t)$, the polynomial $A_m^2(z,t)$ is a very close "approximation" to the polynomial $A_{m+1}(z,t)$ that we are actually looking for next, which is only "off" by a factor of 2. In practice, one can recursively compute polynomials $A_\delta(z,t)$ satisfying (2.11) by following the procedure outlined in the next-to-last paragraph before Lemma 6 in the next section. It is these computations (part of which are reported in Proposition 2) which have led us to believe in the truth of Conjecture 4.

3 Coefficient extraction from powers of $\Phi(z)$

In the next section we are going to describe a method for expressing formal power series satisfying certain differential equations, after the coefficients of the series have been reduced modulo 2^k, as polynomials in the 2-power series $\Phi(z)$ (which has been discussed in the previous section; for the definition see (1.1)), the coefficients being Laurent polynomials in z. Such a method would be without value if we could not, at the same time, provide a procedure for extracting coefficients from powers of $\Phi(z)$. The description of such a procedure is the topic of this section.

Clearly, a brute force expansion of a power $\Phi^K(z)$, where K is a given positive integer, yields

$$\Phi^K(z) = \sum_{r=1}^{K} \sum_{\substack{a_1,\ldots,a_r \geq 1 \\ a_1+\cdots+a_r=K}} \frac{K!}{a_1!\, a_2! \cdots a_r!} H_{a_1,a_2,\ldots,a_r}(z), \tag{3.1}$$

where

$$H_{a_1,a_2,\ldots,a_r}(z) := \sum_{n_1>n_2>\cdots>n_r\geq 0} z^{a_1 2^{n_1}+a_2 2^{n_2}+\cdots+a_r 2^{n_r}}.$$

The expansion (3.1) is not (yet) suited for our purpose, since, when $a_1, a_2, \ldots, a_r$ vary over all possible choices such that their sum is K, the series $H_{a_1,a_2,\ldots,a_r}(z)$ are *not* linearly independent over the ring $\mathbb{Z}[z,z^{-1}]$ of Laurent polynomials in z over the integers[1], and, second, coefficient extraction from a series $H_{a_1,a_2,\ldots,a_r}(z)$ can be a hairy task if some of the a_i's are even.

However, we shall show (see Corollary 7) that, if we restrict to *odd* a_i's, then the corresponding series $H_{a_1,a_2,\ldots,a_r}(z)$, together with the (trivial) series 1, *are* linearly independent over $\mathbb{Z}[z,z^{-1}]$, and there is an efficient algorithm to express all other series $H_{b_1,b_2,\ldots,b_s}(z)$, where we do *not* make any restriction on the b_i's, as a linear combination over $\mathbb{Z}[z,z^{-1}]$ of 1 and the former series (see Lemma 9). Since coefficient extraction from a series $H_{a_1,a_2,\ldots,a_r}(z)$ with all a_i's odd is straightforward (see Remark 8), this solves the problem of coefficient extraction from powers of $\Phi(z)$.

As a side result, the procedure which we described in the previous paragraph, and which will be substantiated below, provides all the means for determining minimal polynomials in the sense of Section 2: as explained in Item (2) of Remark 5 at the end of that

[1]The same is true for an arbitrary ring in place of the ring $\mathbb{Z}$ of integers.

section, it suffices to find a minimal polynomial for the modulus $2^{2^{\delta}-1}$, $\delta = 1, 2, \ldots$. For doing this, we would take a minimal polynomial $A_{\delta-1}(z,t)$ for the modulus $2^{2^{\delta-1}-1}$, expand the square $A_{\delta-1}^2(z,t)$, and replace each coefficient $c_{\alpha,\beta}$ of a monomial $z^\alpha t^\beta$ in $A_{\delta-1}^2(z,t)$ by $c_{\alpha,\beta} + 2^{2^{\delta}-2}x_{\alpha,\beta}$, where $x_{\alpha,\beta}$ is a variable, thereby obtaining a modified polynomial, $B_{\delta-1}(z,t)$ say. Now we would substitute $\Phi(z)$ for t, so that we obtain $B_{\delta-1}(z,\Phi(z))$. Here, we express powers of $\Phi(z)$ in terms of the series $H_{a_1,a_2,\ldots,a_r}(z)$ with all a_i's being odd, and collect terms. By reading the coefficients of $z^\gamma H_{a_1,a_2,\ldots,a_r}(z)$ in this expansion of $B_{\delta-1}(z,\Phi(z))$ and equating them to zero modulo $2^{2^{\delta}-1}$, we produce a system of linear equations modulo $2^{2^{\delta}-1}$ in the unknowns $x_{\alpha,\beta}$. By the definition of $A_{\delta-1}(z,t)$, after division by $2^{2^{\delta}-2}$, this system reduces to a system modulo 2, that is, to a linear system of equations over the field with two elements. A priori, this system need not have a solution, but experience seems to indicate that it always does; see Conjecture 4.

We start with an auxiliary result pertaining to the uniqueness of representations of integers as sums of powers of 2 with multiplicities, tailor-made for application to the series $H_{a_1,a_2,\ldots,a_r}(z)$.

Lemma 6. *Let d, r, s be positive integers with $r \geq s$, c an integer with $|c| \leq d$, and let $a_1, a_2, \ldots, a_r$ respectively $b_1, b_2, \ldots, b_s$ be two sequences of odd integers, with $1 \leq a_i \leq d$ for $1 \leq i \leq r$, and $1 \leq b_i \leq d$ for $1 \leq i \leq s$. If*

$$a_1 2^{2rd} + a_2 2^{2(r-1)d} + \cdots + a_r 2^{2d} = b_1 2^{n_1} + b_2 2^{n_2} + \cdots + b_s 2^{n_s} + c \tag{3.2}$$

for integers $n_1, n_2, \ldots, n_s$ with $n_1 > n_2 > \cdots > n_s \geq 0$, then $r = s$, $c = 0$, $a_i = b_i$, and $n_i = 2d(r+1-i)$ for $i = 1, 2, \ldots, r$.

Proof. We use induction on r.

First, let $r = 1$. Then $s = 1$ as well, and (3.2) becomes

$$a_1 2^{2d} = b_1 2^{n_1} + c. \tag{3.3}$$

If $n_1 > 2d$, then the above equation, together with the assumption that a_1 is odd, implies

$$2^{2d} \equiv c \mod 2^{2d+1}.$$

However, by assumption, we have $|c| \leq d < 2^{2d}$, which is absurd.

If $d < n_1 < 2d$, then it follows from (3.3) that c must be divisible by 2^{n_1}. Again by assumption, we have $|c| \leq d < 2^d < 2^{n_1}$, so that $c = 0$. But then (3.3) cannot be satisfied since b_1 is assumed to be odd.

If $0 \leq n_1 \leq d$, then we estimate

$$b_1 2^{n_1} + c \leq d\left(2^d + 1\right) \leq (2^d - 1)(2^d + 1) < 2^{2d},$$

which is again a contradiction to (3.3).

The only remaining possibility is $n_1 = 2d$. If this is substituted in (3.3) and the resulting equation is combined with $|c| \leq d < 2^{2d}$, then the conclusion is that the equation can only be satisfied if $c = 0$ and $a_1 = b_1$, in accordance with the assertion of the lemma.

We now perform the induction step. We assume that the assertion of the lemma is established for all $r < R$, and we want to show that this implies its validity for $r = R$. Let t be maximal such that $n_t \geq 2d$. Then reduction of (3.2) modulo 2^{2d} yields

$$b_{t+1}2^{n_{t+1}} + b_{t+2}2^{n_{t+2}} + \cdots + b_s 2^{n_s} + c \equiv 0 \quad \text{modulo } 2^{2d}. \tag{3.4}$$

Let us write $b \cdot 2^{2d}$ for the left-hand side in (3.4). Then, by dividing (3.2) (with R instead of r) by 2^{2d}, we obtain

$$a_1 2^{2(R-1)d} + a_2 2^{2(R-2)d} + \cdots + a_{R-1}2^{2d} = b_1 2^{n_1-2d} + b_2 2^{n_2-2d} + \cdots + b_t 2^{n_t-2d} + b - a_R. \tag{3.5}$$

We have

$$\begin{aligned} 0 \leq b &\leq 2^{-2d} d \left(2^{2d-1} + 2^{2d-2} + \cdots + 2^{2d-s+t} + 1\right) \\ &\leq 2^{-2d} d \left(2^{2d} - 2^{2d-s+t} + 1\right) \leq d. \end{aligned}$$

Consequently, we also have $|b - a_R| \leq d$. This means that we are in a position to apply the induction hypothesis to (3.5). The conclusion is that $t = R - 1$, $b - a_R = 0$, $a_i = b_i$, and $n_i = 2d(R + 1 - i)$ for $i = 1, 2, \ldots, R - 1$. If this is used in (3.2) with $r = R$, then we obtain

$$a_R 2^{2d} = c$$

or

$$a_R 2^{2d} = b_R 2^{n_R} + c,$$

depending on whether $s = R - 1$ or $s = R$. The first case is absurd since $c \leq d < 2^{2d} \leq a_R 2^{2d}$. On the other hand, the second case has already been considered in (3.3), and we have seen there that it follows that $c = 0$, $a_R = b_R$, and $n_R = 2d$.

This completes the proof of the lemma. □

The announced independence of the series $H_{a_1,a_2,\ldots,a_r}(z)$ with all a_i's odd is now an easy consequence.

Corollary 7. *The series $H_{a_1,a_2,\ldots,a_r}(z)$, with all a_i's odd, together with the series 1 are linearly independent over $(\mathbb{Z}/2\mathbb{Z})[z, z^{-1}]$, and consequently as well over $(\mathbb{Z}/2^\gamma\mathbb{Z})[z, z^{-1}]$ for an arbitrary positive integer γ, and over $\mathbb{Z}[z, z^{-1}]$.*

Proof. Let us suppose that

$$p_0(z) + \sum_{i=1}^{N} p_i(z) H_{a_1^{(i)},a_2^{(i)},\ldots,a_{r_i}^{(i)}}(z) = 0, \tag{3.6}$$

where the $p_i(z)$'s are non-zero Laurent polynomials in z over $\mathbb{Z}/2\mathbb{Z}$ (respectively over $\mathbb{Z}/2^\gamma\mathbb{Z}$ or over $\mathbb{Z}$), the r_i's are positive integers, and $a_j^{(i)}$, $j = 1, 2, \ldots, r_i$, $i = 1, 2, \ldots, N$, are odd integers. We may also assume that the tuples $(a_1^{(i)}, a_2^{(i)}, \ldots, a_{r_i}^{(i)})$, $i = 1, 2, \ldots, N$, are pairwise distinct. Choose i_0 such that r_{i_0} is maximal among the r_i's. Without loss

of generality, we may assume that the coefficient of z^0 in $p_{i_0}(z)$ is non-zero (otherwise we could multiply both sides of (3.6) by an appropriate power of z). Let d be the maximum of all $a_j^{(i)}$'s and the absolute values of exponents of z appearing in monomials with non-zero coefficient in the Laurent polynomials $p_i(z)$, $i = 0, 1, \dots, N$. Then, according to Lemma 6 with $r = r_{i_0}$, $a_j = a_j^{(i_0)}$, $j = 1, 2, \dots, r_{i_0}$, the coefficient of

$$z^{a_1^{(i_0)}2^{2rd}+a_2^{(i_0)}2^{2(r-1)d}+\cdots+a_r^{(i_0)}2^{2d}}$$

is 1 in $H_{a_1^{(i_0)},a_2^{(i_0)},\dots,a_{r_{i_0}}^{(i_0)}}(z)$, while it is zero in series $z^e H_{a_1^{(i_0)},a_2^{(i_0)},\dots,a_{r_{i_0}}^{(i_0)}}(z)$, where e is a non-zero integer with $|e| \le d$, and in all other series $z^e H_{a_1^{(i)},a_2^{(i)},\dots,a_{r_i}^{(i)}}(z)$, $i = 1, \dots, i_0 - 1, i_0 + 1, \dots, N$, where e is a (not necessarily non-zero) integer with $|e| \le d$. This contradiction to (3.6) establishes the assertion of the corollary. □

Remark 8. Coefficient extraction from a series $H_{a_1,a_2,\dots,a_r}(z)$ with all a_i's odd is straightforward: if we want to know whether z^M appears in $H_{a_1,a_2,\dots,a_r}(z)$, that is, whether we can represent M as

$$M = a_1 2^{n_1} + a_2 2^{n_2} + \cdots + a_r 2^{n_r}$$

for some $n_1, n_2, \dots, n_r$ with $n_1 > n_2 > \cdots > n_r \ge 0$, then necessarily $n_r = v_2(M)$, $n_{r-1} = v_2(M - a_r 2^{n_r})$, etc. The term z^M appears in $H_{a_1,a_2,\dots,a_r}(z)$ if, and only if, the above process terminates after *exactly* r steps. This means, that, with $n_r, n_{r-1}, \dots, n_1$ constructed as above, we have

$$M - (a_s 2^{n_s} + \cdots + a_{r-1} 2^{n_{r-1}} + a_r 2^{n_r}) > 0$$

for $s > 1$, and

$$M - (a_1 2^{n_1} + \cdots + a_{r-1} 2^{n_{r-1}} + a_r 2^{n_r}) = 0.$$

It should be noted that, given $a_1, a_2, \dots, a_r$, this procedure of coefficient extraction needs at most $O(\log M)$ operations, that is, its computational complexity is linear.

Our next goal is to show that a series $H_{b_1,b_2,\dots,b_s}(z)$ can be expressed as a linear combination over $\mathbb{Z}[z, z^{-1}]$ of the series 1 and the series $H_{a_1,a_2,\dots,a_r}(z)$, where all a_i's are odd. In doing this, we are forced to consider the more general series

$$H_{b_1,b_2,\dots,b_s}^{\beta_1,\beta_2,\dots,\beta_s}(z) := \sum_{n_1+\beta_1 > n_2+\beta_2 > \cdots > n_s+\beta_s \ge 0} z^{b_1 2^{n_1} + b_2 2^{n_2} + \cdots + b_s 2^{n_s}},$$

where, as before, $b_1, b_2, \dots, b_s$ are positive integers, and $\beta_1, \beta_2, \dots, \beta_s$ are integers.

Lemma 9. *For positive integers $b_1, b_2, \dots, b_s$ and integers $\beta_1, \beta_2, \dots, \beta_s$, the series $H_{b_1,b_2,\dots,b_s}^{\beta_1,\beta_2,\dots,\beta_s}(z)$ can be expressed as a linear combination over $\mathbb{Z}[z^{1/2^e}]$ (for a suitable integer e) of the series 1 and series of the form $H_{a_1,a_2,\dots,a_r}(z)$, where all a_i's are odd. Moreover, in the above expansion of the series $H_{b_1,b_2,\dots,b_s}(z) = H_{b_1,b_2,\dots,b_s}^{0,0,\dots,0}(z)$ we have $e = 0$; that is, in that case all coefficients are in $\mathbb{Z}[z]$.*

Proof. We describe an algorithmic procedure for expressing $H^{\beta_1,\beta_2,\ldots,\beta_s}_{b_1,b_2,\ldots,b_s}(z)$ in terms of series $H^{\gamma_1,\gamma_2,\ldots,\gamma_r}_{a_1,a_2,\ldots,a_r}(z)$, where either $r < s$, or $r = s$ and

$$\max\{i : a_i \text{ is even or } \gamma_i \neq 0\} < \max\{i : b_i \text{ is even or } \beta_i \neq 0\}.$$

In words, in the second case the length of the string of consecutive 0's at the tail of the upper parameters respectively the length of the string of consecutive odd numbers at the tail of the lower parameters has been increased.

Our algorithmic procedure consists of four recurrence relations, (3.7)–(3.10) below. For the first two of these, let $b_s = b'_s 2^{e_s}$, where $e_s = v_2(b_s)$. By definition, the number b'_s is odd. Then we have

$$H^{\beta_1,\beta_2,\ldots,\beta_s}_{b_1,b_2,\ldots,b_s}(z) = \sum_{n_1+\beta_1-\beta_s+e_s>\cdots>n_{s-1}+\beta_{s-1}-\beta_s+e_s>n_s+e_s\geq-\beta_s+e_s} z^{b_1 2^{n_1}+b_2 2^{n_2}+\cdots+b_{s-1}2^{n_{s-1}}+b'_s 2^{n_s+e_s}}.$$

In the above sum on the right-hand side, let $n'_s = n_s + e_s$ be a new summation index. Then, for $e_s \leq \beta_s$, one sees that

$$H^{\beta_1,\beta_2,\ldots,\beta_s}_{b_1,b_2,\ldots,b_s}(z) = H^{\beta_1-\beta_s+e_s,\beta_2-\beta_s+e_s,\ldots,\beta_{s-1}-\beta_s+e_s,0}_{b_1,b_2,\ldots,b_{s-1},b'_s}(z) + \sum_{k=1}^{\beta_s-e_s} z^{b'_s 2^{-k}} H^{\beta_1-\beta_s+e_s+k-1,\beta_2-\beta_s+e_s+k-1,\ldots,\beta_{s-1}-\beta_s+e_s+k-1}_{b_1,b_2,\ldots,b_{s-1}}(z). \quad (3.7)$$

On the other hand, for $e_s \geq \beta_s$, one has

$$H^{\beta_1,\beta_2,\ldots,\beta_s}_{b_1,b_2,\ldots,b_s}(z) = H^{\beta_1-\beta_s+e_s,\beta_2-\beta_s+e_s,\ldots,\beta_{s-1}-\beta_s+e_s,0}_{b_1,b_2,\ldots,b_{s-1},b'_s}(z) - \sum_{k=0}^{e_s-\beta_s-1} z^{b'_s 2^{k}} H^{\beta_1-\beta_s+e_s-k-1,\beta_2-\beta_s+e_s-k-1,\ldots,\beta_{s-1}-\beta_s+e_s-k-1}_{b_1,b_2,\ldots,b_{s-1}}(z). \quad (3.8)$$

Now consider

$$H^{\beta_1,\ldots,\beta_h,0,\ldots,0}_{b_1,\ldots,b_h,b_{h+1},\ldots,b_s}(z),$$

where $1 \leq h < s$ and all of $b_{h+1}, \ldots, b_s$ are odd. Similar to the proceedings above, let $b_h = b'_h 2^{e_h}$, where $e_h = v_2(b_h)$. Again, by definition, the number b'_h is odd. Then we have

$$H^{\beta_1,\ldots,\beta_h,0,\ldots,0}_{b_1,\ldots,b_h,b_{h+1},\ldots,b_s}(z) = \sum_{\substack{n_1+\beta_1-\beta_h+e_h>\cdots>n_{h-1}+\beta_{h-1}-\beta_h+e_h>n_h+e_h \\ n_h+\beta_h>n_{h+1}>\cdots>n_s\geq 0}} z^{b_1 2^{n_1}+\cdots+b_{h-1}2^{n_{h-1}}+b'_h 2^{n_h+e_h}+b_{h+1}2^{n_{h+1}}+\cdots+b_s 2^{n_s}}.$$

In the above sum on the right-hand side, let $n'_h = n_h + e_h$ be a new summation index. Then, for $e_h \le \beta_h$, one sees that

$$H^{\beta_1,\dots,\beta_h,0,\dots,0}_{b_1,\dots,b_h,b_{h+1},\dots,b_s}(z) = H^{\beta_1-\beta_h+e_h,\dots,\beta_{h-1}-\beta_h+e_h,0,0,\dots,0}_{b_1,\dots,b_{h-1},b'_h,b_{h+1},\dots,b_s}(z) + \sum_{k=0}^{\beta_h-e_h-1} H^{\beta_1-\beta_h+e_h+k,\dots,\beta_{h-1}-\beta_h+e_h+k,k,0,\dots,0}_{b_1,\dots,b_{h-1},b'_h+b_{h+1}2^k,b_{h+2},\dots,b_s}(z). \quad (3.9)$$

On the other hand, for $e_h \ge \beta_h$, one has

$$H^{\beta_1,\dots,\beta_h,0,\dots,0}_{b_1,\dots,b_h,b_{h+1},\dots,b_s}(z) = H^{\beta_1-\beta_h+e_h,\dots,\beta_{h-1}-\beta_h+e_h,0,0,\dots,0}_{b_1,\dots,b_{h-1},b'_h,b_{h+1},\dots,b_s}(z) - \sum_{k=1}^{e_h-\beta_h} H^{\beta_1-\beta_h+e_h-k,\dots,\beta_{h-1}-\beta_h+e_h-k,0,0,\dots,0}_{b_1,\dots,b_{h-1},b'_h2^k+b_{h+1},b_{h+2},\dots,b_s}(z). \quad (3.10)$$

It is clear that, if we recursively apply (3.7)–(3.10) to a given series $H^{\beta_1,\beta_2,\dots,\beta_s}_{b_1,b_2,\dots,b_s}(z)$, and use $H^{\emptyset}_{\emptyset}(z) = 1$ as an initial condition, we will eventually arrive at a linear combination of 1 and series $H^{0,0,\dots,0}_{a_1,a_2,\dots,a_r}(z) = H_{a_1,a_2,\dots,a_r}(z)$ with all a_i's being odd, where the coefficients are polynomials in $z^{1/2^e}$ for a suitable e. (Potential fractional exponents come from the relation (3.7).) This proves the first assertion of the lemma.

Now let us consider the case where all the β_i's are zero. Suppose that we have an expansion as described in the first part of the lemma for $H_{b_1,b_2,\dots,b_s}(z)$,

$$H_{b_1,b_2,\dots,b_s}(z) = \sum_{\mathbf{a}} c(\mathbf{a}) z^{e(\mathbf{a})} H_{\mathbf{a}}(z), \quad (3.11)$$

where the sum is taken over all finite tuples $\mathbf{a} = (a_1, a_2, \dots)$ with all a_i's being odd, and where only finitely many coefficients $c(\mathbf{a})$ are non-zero. We also allow the tuple $\mathbf{a}$ to be the empty tuple () and make the convention that $H_{()}(z) = 1$, so that the series 1 is as well included in the linear combination on the right-hand side of (3.11).

Let us now consider exponents $e(\mathbf{a})$ that are not integral. Let ϵ be a real number strictly between 0 and 1, and concentrate on exponents $e(\mathbf{a})$ with fractional part ϵ; in symbols $\{e(\mathbf{a})\} = \epsilon$. Then we isolate these exponents $e(\mathbf{a})$ in the relation (3.11), and since there are no fractional exponents on the left-hand side, we obtain

$$0 = \sum_{\{e(\mathbf{a})\}=\epsilon} c(\mathbf{a}) z^{e(\mathbf{a})} H_{\mathbf{a}}(z).$$

After dividing both sides through by z^{ϵ}, an application of Corollary 7 shows that $c(\mathbf{a}) = 0$ for all $\mathbf{a}$ with $\{e(\mathbf{a})\} = \epsilon$. Thus, all exponents $e(\mathbf{a})$ actually occurring in (3.11) with non-zero coefficients $c(\mathbf{a})$ are in fact integral. This completes the proof of the lemma. □

Computer computations suggest that, if we restrict our attention to the series $H_{b_1,b_2,\dots,b_s}(z)$, which are the ones that we are actually interested in, there is a strengthening of Lemma 9 (see also Appendix A).

Conjecture 10. *For any positive integers $b_1, b_2, \dots, b_s$, the series $H_{b_1,b_2,\dots,b_s}(z)$ can be expressed as a linear combination over $\mathbb{Z}[z, z^{-1}]$ of the series 1 and series of the form $H_{a_1,a_2,\dots,a_r}(z)$, where all a_i's are odd, $r \le s$, and $a_1 + a_2 + \cdots + a_r \le b_1 + b_2 + \cdots + b_s$.*

To conclude this section, let us provide an illustration of the above discussion. We set ourselves the task of determining the coefficient of $z^{1099511640192}$ in $\Phi^5(z)$. In order to accomplish this task, we first express $\Phi^5(z)$ in terms of series $H_{a_1,\dots,a_r}(z)$ with all a_i's being odd. This is done by means of the expansion (3.1) and the algorithm described in the proof of Lemma 9. The resulting expansion is displayed in Appendix A.

Now we have to answer the question, in which of the series $H_{a_1,\dots,a_r}(z)$ that appear in this expansion of $\Phi^5(z)$ do we find the monomial $z^{1099511640192}$. Using the algorithm described in Remark 8, we see that

$$\begin{aligned}
1099511640192 &= 5 \cdot 2^7 + 1099511639552,\\
&= 3 \cdot 2^{13} + 2^{12} + 2^7 + 1099511611392,\\
&= 2^{40} + 3 \cdot 2^{12} + 2^7,\\
&= 2^9 + 2^8 + 3 \cdot 2^7 + 1099511639040,\\
&= 3 \cdot 2^{12} + 2^7 + 1099511627776,\\
&= 2^8 + 3 \cdot 2^7 + 1099511639552,\\
&= 2^{40} + 2^{13} + 2^{12} + 2^7,\\
&= 1 + 3 \cdot 2^0 + 1099511640188,\\
&= 3 \cdot 2^7 + 1099511639808,\\
&= 1 + 2^2 + 2^1 + 2^0 + 1099511640184,\\
&= 2^{13} + 2^{12} + 2^7 + 1099511627776,\\
&= 1 + 2^1 + 2^0 + 1099511640188,\\
&= 2^{12} + 2^7 + 1099511635968,\\
&= 2 + 2^1 + 1099511640188,\\
&= 1 + 2^0 + 1099511640190,\\
&= 2^7 + 1099511640064.
\end{aligned}$$

Here, the third line shows that $z^{1099511640192}$ appears in $H_{1,3,1}(z)$, and the seventh line shows that it appears in $H_{1,1,1,1}(z)$ (thereby making it impossible to appear in $H_{1,1,1,1,1}(z)$), while the remaining lines show that it does not appear in any other term in the expansion of $\Phi^5(z)$ displayed in Appendix A. Hence, by taking into account the coefficients with which the series $H_{1,3,1}(z)$ and $H_{1,1,1,1}(z)$ appear in this expansion, the coefficient of $z^{1099511640192}$ in $\Phi^5(z)$ is seen to equal $-40 + 240 = 200$.

4 The method

We consider a (formal) differential equation

$$\mathcal{P}(z; F(z), F'(z), F''(z), \dots, F^{(s)}(z)) = 0, \tag{4.1}$$

where $\mathcal{P}$ is a polynomial with integer coefficients, which has a power series solution $F(z)$ with integer coefficients. In this situation, we propose the following algorithmic approach to determining the series $F(z)$ modulo a 2-power $2^{3\cdot 2^\alpha}$, for some positive integer α. We make the Ansatz

$$F(z) = \sum_{i=0}^{2^{\alpha+2}-1} a_i(z)\Phi^i(z) \quad \text{modulo } 2^{3\cdot 2^\alpha}, \tag{4.2}$$

with $\Phi(z)$ as given in (1.1), and where the $a_i(z)$'s are (at this point) undetermined Laurent polynomials in z. Now we substitute (4.2) into (4.1), and we shall gradually determine approximations $a_{i,\beta}(z)$ to $a_i(z)$ such that (4.1) holds modulo 2^β, for $\beta = 1, 2, \ldots, 3\cdot 2^\alpha$. To start the procedure, we consider the differential equation (4.1) modulo 2, with

$$F(z) = \sum_{i=0}^{2^{\alpha+2}-1} a_{i,1}(z)\Phi^i(z) \quad \text{modulo } 2. \tag{4.3}$$

Using the elementary fact that $\Phi'(z) = 1$ modulo 2, we see that the left-hand side of (4.1) is a polynomial in $\Phi(z)$ with coefficients that are Laurent polynomials in z. We reduce powers $\Phi^k(z)$ with $k \geq 2^{\alpha+2}$ using the relation (which is implied by the minimal polynomial for the modulus 8 given in Proposition 2) [2]

$$\left(\Phi^4(z) + 6\Phi^3(z) + (2z+3)\Phi^2(z) + (2z+6)\Phi(z) + 2z + 5z^2\right)^{2^\alpha} = 0 \quad \text{modulo } 2^{3\cdot 2^\alpha}. \tag{4.4}$$

Since, at this point, we are only interested in finding a solution to (4.1) modulo 2, the above relation simplifies to

$$\Phi^{2^{\alpha+2}}(z) + \Phi^{2^{\alpha+1}}(z) + z^{2^{\alpha+1}} = 0 \quad \text{modulo } 2. \tag{4.5}$$

Now we compare coefficients of powers $\Phi^k(z)$, $k = 0, 1, \ldots, 2^{\alpha+2}-1$ (see Remark 11). This yields a system of $2^{\alpha+2}$ (differential) equations (modulo 2) for the unknown Laurent polynomials $a_{i,1}(z)$, $i = 0, 1, \ldots, 2^{\alpha+2}-1$, which may or may not have a solution.

Provided we have already found Laurent polynomials $a_{i,\beta}(z)$, $i = 0, 1, \ldots, 2^{\alpha+2}-1$, for some β with $1 \leq \beta \leq 3\cdot 2^\alpha - 1$, such that

$$\sum_{i=0}^{2^{\alpha+2}-1} a_{i,\beta}(z)\Phi^i(z) \tag{4.6}$$

[2] Actually, if we would like to obtain an optimal result, we should use the relation implied by a minimal polynomial for the modulus $2^{3\cdot 2^\alpha}$ in the sense of Section 2. But since we have no general formula available for such a minimal polynomial (cf. Item (2) of Remark 5 in that section), and since we wish to prove results for arbitrary moduli, choosing instead powers of a minimal polynomial for the modulus 8 is the best compromise. In principle, it may happen that there exists a polynomial in $\Phi(z)$ with coefficients that are Laurent polynomials in z, which is identical with $F(z)$ after reduction of its coefficients modulo $2^{3\cdot 2^\alpha}$, but the Ansatz (4.2) combined with the reduction (4.4) fails because it is too restrictive. We are not aware of a concrete example where this obstruction occurs. The subgroup numbers of $SL_2(\mathbb{Z})$ (which we treat modulo 8 in Section 11 by the method described here, and modulo 16 by an enhancement of the method outlined in Appendix D) are a potential candidate when considered modulo $2^{3\cdot 2^\alpha}$ for $\alpha \geq 1$. On the other hand, once we are successful using this (potentially problematic) Ansatz, then the result can easily be converted into an optimal one by further reducing the polynomial thus obtained, using the relation implied by a minimal polynomial for the modulus $2^{3\cdot 2^\alpha}$.

solves (4.1) modulo 2^β, we put

$$a_{i,\beta+1}(z) := a_{i,\beta}(z) + 2^\beta b_{i,\beta+1}(z), \quad i = 0, 1, \ldots, 2^{\alpha+2} - 1, \tag{4.7}$$

where the $b_{i,\beta+1}(z)$'s are (at this point) undetermined Laurent polynomials in z. Next we substitute

$$\sum_{i=0}^{2^{\alpha+2}-1} a_{i,\beta+1}(z)\Phi^i(z) \tag{4.8}$$

instead of $F(z)$ in (4.1). Using the fact that $\Phi'(z) = \sum_{n=0}^{\beta} 2^n z^{2^n-1}$ modulo $2^{\beta+1}$, we expand the left-hand side as a polynomial in $\Phi(z)$ (with coefficients being Laurent polynomials in z), we apply again the reduction using relation (4.4), we compare coefficients of powers $\Phi^k(z)$, $k = 0, 1, \ldots, 2^{\alpha+2} - 1$ (again, see Remark 11), and, as a result, we obtain a system of $2^{\alpha+2}$ (differential) equations (modulo $2^{\beta+1}$) for the unknown Laurent polynomials $b_{i,\beta+1}(z)$, $i = 0, 1, \ldots, 2^{\alpha+2} - 1$, which may or may not have a solution. If we manage to push this procedure through until $\beta = 3 \cdot 2^\alpha - 1$, then, setting $a_i(z) = a_{i,3\cdot 2^\alpha}(z)$, $i = 0, 1, \ldots, 2^{\alpha+2} - 1$, the right-hand side of (4.2) is a solution to (4.1) modulo $2^{3\cdot 2^\alpha}$, as required.

Remark 11. As the reader will have noticed, each comparison of coefficients of powers of $\Phi(z)$ is based on the "hope" that, if a polynomial in $\Phi(z)$ is zero modulo a 2-power 2^β (as a formal Laurent series), then already all coefficients of powers of $\Phi(z)$ in this polynomial vanish modulo 2^β. However, this implication is false in general (see Lemma 39 below for the case of modulus $2^4 = 16$). It may thus happen that the method described in this section fails to find a solution modulo 2^β to a given differential equation in the form of a polynomial in $\Phi(z)$ with coefficients that are Laurent polynomials in z over the integers, while such a solution does in fact exist. As a matter of fact, this situation occurs in the analysis modulo 16 of the subgroup numbers of $SL_2(\mathbb{Z})$, see Theorem 28. In Appendix D, we outline an enhancement of the method, which (at least in principle; Appendix D treats only the case of the modulus 16 explicitly) allows us to decide whether or not a solution modulo a given power in terms of a polynomial in $\Phi(z)$ with coefficients that are Laurent polynomials in z over the integers exists, and, if so, to explicitly find such a solution.

It is not difficult to see that performing the iterative step (4.7) amounts to solving a system of linear differential equations in the unknown functions $b_{i,\beta+1}(z)$ modulo 2, where all of them are Laurent polynomials in z, and where only first derivatives of the $b_{i,\beta+1}(z)$'s occur. Solving such a system is equivalent to solving an ordinary system of linear equations, as is shown by the lemma below.

Given a Laurent polynomial $p(z)$ over the integers, we write $p^{(o)}(z)$ for the odd part $\frac{1}{2}(p(z) - p(-z))$ and $p^{(e)}(z)$ for the even part $\frac{1}{2}(p(z) + p(-z))$ of $p(z)$, respectively.

Lemma 12. *Let $c_{i,j}(z)$ and $d_{i,j}(z)$, $1 \le i, j \le N$, and $r_i(z)$, $1 \le i \le N$, be given Laurent polynomials in z with integer coefficients. Then the system of differential equations*

$$\sum_{j=1}^{N} c_{i,j}(z) f_j(z) + \sum_{j=1}^{N} d_{i,j}(z) f_j'(z) = r_i(z) \quad \text{modulo } 2, \qquad 1 \le i \le N, \tag{4.9}$$

has solutions $f_j(z)$, $1 \le j \le N$, *that are Laurent polynomials in* z *over the integers if, and only if, the system of* linear *equations*

$$\begin{aligned}
&\sum_{j=1}^{N} c_{i,j}^{(e)}(z) f_j^{(1)}(z) + \sum_{j=1}^{N} c_{i,j}^{(o)}(z) f_j^{(2)}(z) + \sum_{j=1}^{N} z^{-1} d_{i,j}^{(1)}(z) f_j^{(2)}(z) = r_i^{(e)}(z) \quad \text{modulo 2,} \\
&\sum_{j=1}^{N} c_{i,j}^{(o)}(z) f_j^{(1)}(z) + \sum_{j=1}^{N} c_{i,j}^{(e)}(z) f_j^{(2)}(z) + \sum_{j=1}^{N} z^{-1} d_{i,j}^{(o)}(z) f_j^{(2)}(z) = r_i^{(o)}(z) \quad \text{modulo 2,} \\
&\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad 1 \le i \le N,
\end{aligned} \tag{4.10}$$

has a solution in Laurent polynomials $f_j^{(1)}(z), f_j^{(2)}(z)$ *in* z *over the integers for* $1 \le j \le N$.

Proof. We write $f_j(z) = f_j^{(e)}(z) + f_j^{(o)}(z)$, and observe that

$$f_j'(z) = z^{-1} f_j^{(o)}(z) \quad \text{modulo 2.}$$

If this is used in (4.9), and if we separate the even and odd parts on both sides of the equations, then (4.10) with $f_j^{(1)}(z) = f_j^{(e)}(z)$ and $f_j^{(2)}(z) = f_j^{(o)}(z)$, $j = 1, 2, \ldots, N$, results after little manipulation.

Conversely, suppose that $g_j^{(1)}(z), g_j^{(2)}(z)$, $j = 1, 2, \ldots, N$, is a solution to the system (4.10), that is,

$$\begin{aligned}
&\sum_{j=1}^{N} c_{i,j}^{(e)}(z) g_j^{(1)}(z) + \sum_{j=1}^{N} c_{i,j}^{(o)}(z) g_j^{(2)}(z) + \sum_{j=1}^{N} z^{-1} d_{i,j}^{(1)}(z) g_j^{(2)}(z) = r_i^{(e)}(z) \quad \text{modulo 2,} \\
&\sum_{j=1}^{N} c_{i,j}^{(o)}(z) g_j^{(1)}(z) + \sum_{j=1}^{N} c_{i,j}^{(e)}(z) g_j^{(2)}(z) + \sum_{j=1}^{N} z^{-1} d_{i,j}^{(o)}(z) g_j^{(2)}(z) = r_i^{(o)}(z) \quad \text{modulo 2,} \\
&\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad 1 \le i \le N.
\end{aligned} \tag{4.11}$$

At this point, the $g_j^{(1)}(z)$'s need not be even Laurent polynomials, and the $g_j^{(2)}(z)$'s need not be odd Laurent polynomials. We have to prove that there exists a solution $f_j^{(1)}(z), f_j^{(2)}(z)$, $j = 1, 2, \ldots, N$, such that all $f_j^{(1)}(z)$'s are even Laurent polynomials and all $f_j^{(2)}(z)$'s are odd Laurent polynomials.

By separating even and odd parts of the $g_k^{(1)}(z)$'s and the $g_j^{(2)}(z)$'s, we obtain the

equations

$$\sum_{j=1}^{N} c_{i,j}^{(e)}(z)(g_j^{(1)})^{(e)}(z) + \sum_{j=1}^{N} c_{i,j}^{(o)}(z)(g_j^{(2)})^{(o)}(z) + \sum_{j=1}^{N} z^{-1} d_{i,j}^{(1)}(z)(g_j^{(2)})^{(o)}(z) = r_i^{(e)}(z)$$

$$\text{modulo 2,} \quad (4.12)$$

$$\sum_{j=1}^{N} c_{i,j}^{(e)}(z)(g_j^{(1)})^{(o)}(z) + \sum_{j=1}^{N} c_{i,j}^{(o)}(z)(g_j^{(2)})^{(e)}(z) + \sum_{j=1}^{N} z^{-1} d_{i,j}^{(1)}(z)(g_j^{(2)})^{(e)}(z) = 0$$

$$\text{modulo 2,}$$

$$\sum_{j=1}^{N} c_{i,j}^{(o)}(z)(g_j^{(1)})^{(e)}(z) + \sum_{j=1}^{N} c_{i,j}^{(e)}(z)(g_j^{(2)})^{(o)}(z) + \sum_{j=1}^{N} z^{-1} d_{i,j}^{(o)}(z)(g_j^{(2)})^{(o)}(z) = r_i^{(o)}(z)$$

$$\text{modulo 2,} \quad (4.13)$$

$$\sum_{j=1}^{N} c_{i,j}^{(o)}(z)(g_j^{(1)})^{(o)}(z) + \sum_{j=1}^{N} c_{i,j}^{(e)}(z)(g_j^{(2)})^{(e)}(z) + \sum_{j=1}^{N} z^{-1} d_{i,j}^{(o)}(z)(g_j^{(2)})^{(e)}(z) = 0$$

$$\text{modulo 2,}$$

$$1 \le i \le N.$$

Combining (4.12) and (4.13), we see that $(g_j^{(1)})^{(e)}(z), (g_j^{(2)})^{(o)}(z)$, $j = 1, 2, \ldots, N$, is a solution to (4.10), and now the $(g_j^{(1)})^{(e)}(z)$'s are indeed even polynomials while the $(g_j^{(2)})^{(o)}(z)$'s are indeed odd polynomials. Addition of both sides of (4.12) and (4.13) then yields that

$$f_j(z) := (g_j^{(1)})^{(e)}(z) + (g_j^{(2)})^{(o)}(z), \quad 1 \le j \le N,$$

is a solution to (4.9) in Laurent polynomials in z over the integers. □

In general, it is difficult to characterise when the system (4.10) has a solution. What one has to do is to solve the system over the *field* of rational functions in z over $\mathbb{Z}/2\mathbb{Z}$, and then to see whether possibly occurring denominators cancel out or, in the case of a parametric solution, whether denominators can be *made* to cancel by a suitable choice of the parameters. One simple case, where a characterisation is possible, is given in Lemma 22, which is crucial for the proof that the generating function for the number of subgroups of index n of $PSL_2(\mathbb{Z})$, when these are reduced modulo a given power of 2, can always be expressed as a polynomial in $\Phi(z)$ with coefficients that are Laurent polynomials in z.

We remark that the idea of the method that we have described in this section has certainly further potential. For example, the fact that the series $\Phi(z)$ remains invariant under the substitution $z \to z^2$ (or, more generally, under the substitution $z \to z^{2^h}$, where h is some positive integer) — up to a simple additive correction — can be exploited in order to extend the range of applicability of our method to equations where we not

only allow differentiation but also this kind of substitution. This is actually already used in a very hidden way in Section 14 (cf. [27, Theorem 12], setting in relation subgroup numbers of the Hecke group $\mathfrak{H}(q)$ with subgroup numbers of $C_q * C_q$ modulo 2; in terms of generating functions, the meaning of this theorem is that the generating function for the former numbers can be expressed in terms of the generating function for the latter numbers by a relation which involves a substitution $z \to z^2$). Furthermore, as we already mentioned in the introduction, there is no obstacle to modifying the method presented here to work for recursive sequences which are reduced modulo powers of p, in connection with the series $\sum_{n\geq 0} z^{p^n}$, although at present we are not able to offer any interesting applications in this direction.

5 A sample application: Catalan numbers

The *Catalan numbers*, defined by $\mathrm{Cat}_n = \frac{1}{n+1}\binom{2n}{n}$, $n = 0, 1, \ldots$, are ubiquitous in enumerative combinatorics. (Stanley provides a list of 66 sequences of sets enumerated by Catalan numbers in [32, Ex. 6.19], with many more in the addendum [33].) Recently, there have been several papers on the congruence properties of Catalan numbers modulo powers of 2, see [11, 22, 30, 38]. In particular, in [22] the Catalan numbers are determined modulo 64. As we already mentioned in the introduction, the corresponding result (cf. [22, Theorems 6.1–6.6]) can be compactly written in the form (1.2). Clearly, once we know the right-hand side of (1.2), the validity of the congruence (1.2) can be routinely verified by substituting the right-hand side into the well-known functional equation (cf. [36, (2.3.8)])

$$zC^2(z) - C(z) + 1 = 0, \tag{5.1}$$

where $C(z) = \sum_{n=0}^{\infty} \mathrm{Cat}_n\, z^n$ denotes the generating function for the Catalan numbers, and reducing powers of $\Phi(z)$ whose exponent exceeds 7 by means of the relation (4.4) with $\alpha = 1$. We shall now demonstrate that the method from Section 4 allows one not only to *find* the congruence (1.2) algorithmically, but also to find analogous congruences modulo *arbitrary* powers of 2.[3]

Theorem 13. *Let $\Phi(z) = \sum_{n\geq 0} z^{2^n}$, and let α be some positive integer. Then the generating function $C(z)$ for Catalan numbers, reduced modulo $2^{3\cdot 2^\alpha}$, can be expressed as a polynomial in $\Phi(z)$ of degree at most $2^{\alpha+2}-1$ with coefficients that are Laurent polynomials in z over the integers.*

Proof. We apply the method from Section 4. We start by substituting the Ansatz (4.3)

[3] In principle, one could use the generalisations of Lucas' theorem due to Davis and Webb [8], and to Granville [15], respectively, to analyse the classical expression $\frac{1}{n+1}\binom{2n}{n}$ for the Catalan numbers modulo a given 2-power, or, more generally, the right-hand side of (13.2). But this approach would be rather cumbersome in comparison with our method, and it is doubtful that one would be able to derive results which are of the same level of generality as Theorems 13, 14, or 33.

in (5.1) and reducing the result modulo 2. In this way, we obtain

$$z\sum_{i=0}^{2^{\alpha+2}-1} a_{i,1}^2(z)\Phi^{2i}(z) + \sum_{i=0}^{2^{\alpha+2}-1} a_{i,1}(z)\Phi^i(z) + 1 = 0 \quad \text{modulo 2.} \tag{5.2}$$

We may reduce $\Phi^{2i}(z)$ further using the relation (4.5). This leads to

$$\begin{aligned} &z\sum_{i=0}^{2^{\alpha+1}-1} \left(a_{i,1}^2(z) + z^{2^{\alpha+1}} a_{i+2^{\alpha+1},1}^2(z)\right)\Phi^{2i}(z) + z\sum_{i=0}^{2^{\alpha}-1} z^{2^{\alpha+1}} a_{i+3\cdot 2^{\alpha},1}^2(z)\Phi^{2i}(z) \\ &+ z\sum_{i=0}^{2^{\alpha}-1} \left(a_{i+2^{\alpha+1},1}^2(z) + a_{i+3\cdot 2^{\alpha},1}^2(z)\right)\Phi^{2i+2^{\alpha+1}}(z) + \sum_{i=0}^{2^{\alpha+2}-1} a_{i,1}(z)\Phi^i(z) + 1 = 0 \quad \text{modulo 2.} \end{aligned} \tag{5.3}$$

Now we compare coefficients of $\Phi^i(z)$, for $i = 0, 1, \ldots, 2^{\alpha+2}-1$. For i odd, we see immediately that this implies that $a_{i,1}(z) = 0$ modulo 2. Proceeding inductively, we now suppose that $a_{2^\beta u,1}(z) = 0$ modulo 2 for odd u and some positive integer β, $\beta < \alpha$. Reading off coefficients of $\Phi^{2^{\beta+1}i}$, where i is odd, we then obtain

$$\begin{aligned} &z a_{2^\beta i,1}^2(z) + z^{2^{\alpha+1}+1} a_{2^\beta i+2^{\alpha+1},1}^2(z) + z^{2^{\alpha+1}+1} a_{2^\beta i+3\cdot 2^\alpha,1}^2(z) \\ &\qquad + z a_{2^\beta i+2^\alpha,1}^2(z) + z a_{2^\beta i+2^{\alpha+1},1}^2(z) + a_{2^{\beta+1}i,1}(z) = 0 \quad \text{modulo 2.} \end{aligned}$$

However, due to our inductive assumption, all squared terms on the left-hand side of this congruence vanish, and we conclude that $a_{2^{\beta+1}i,1}(z) = 0$ modulo 2.

So far, we have found that all coefficient Laurent polynomials $a_{i,1}(z)$ vanish modulo 2 except possibly $a_{0,1}(z)$ and $a_{2^{\alpha+1},1}(z)$. The corresponding congruences that we obtain from extracting coefficients of $\Phi^0(z)$ and $\Phi^{2^{\alpha+1}}(z)$, respectively, in (5.3), are

$$z a_{0,1}^2(z) + z^{2^{\alpha+1}+1} a_{2^{\alpha+1},1}^2(z) + a_{0,1}(z) + 1 = 0 \quad \text{modulo 2,} \tag{5.4}$$

$$z a_{2^{\alpha+1},1}^2(z) + a_{2^{\alpha+1},1}(z) = 0 \quad \text{modulo 2.} \tag{5.5}$$

The only solutions to (5.5) are $a_{2^{\alpha+1},1}(z) = 0$ modulo 2, respectively $a_{2^{\alpha+1},1}(z) = z^{-1}$ modulo 2. The first option is impossible, since it would imply that, modulo 2, the series $C(z)$ reduces to a polynomial; a contradiction to the well-known fact (easily derivable from Legendre's formula [21, p. 10] for the p-adic valuation of factorials; cf. (2.10)) that the Catalan number Cat_n is odd if, and only if, $n = 2^k - 1$ for some k. Thus,

$$a_{2^{\alpha+1},1}(z) = z^{-1} \quad \text{modulo 2.}$$

Use of this result in (5.4) yields the congruence

$$z a_{0,1}^2(z) + a_{0,1}(z) + z^{2^{\alpha+1}-1} + 1 = 0 \quad \text{modulo 2} \tag{5.6}$$

for $a_{0,1}(z)$. We let

$$a_{0,1}(z) = \widetilde{a}_{0,1}(z) + \sum_{k=0}^{\alpha} z^{2^k-1}$$

and substitute this in (5.6). Thereby, we get

$$z\widetilde{a}_{0,1}^2(z) + \sum_{k=0}^{\alpha} z^{2^{k+1}-1} + \widetilde{a}_{0,1}(z) + \sum_{k=0}^{\alpha} z^{2^k-1} + z^{2^{\alpha+1}-1} + 1 = 0 \quad \text{modulo } 2,$$

or, after simplification,

$$z\widetilde{a}_{0,1}^2(z) + \widetilde{a}_{0,1}(z) = 0 \quad \text{modulo } 2.$$

Again, either $\widetilde{a}_{0,1}(z) = 0$ modulo 2, or $\widetilde{a}_{0,1}(z) = z^{-1}$ modulo 2. Here, the second option is impossible, since it would imply that $C(z)$ contains a negative z-power, which is absurd.

In summary, we have found that

$$a_{0,1}(z) = \sum_{k=0}^{\alpha} z^{2^k-1} \quad \text{modulo } 2,$$

$$a_{2^{\alpha+1},1}(z) = z^{-1} \quad \text{modulo } 2,$$

with all other $a_{i,1}(z)$ vanishing, forms the unique solution modulo 2 in Laurent polynomials $a_{i,1}(z)$ to the system of congruences resulting from (5.3).

After we have completed the "base step," we now proceed with the iterative steps described in Section 4. We consider the Ansatz (4.6)–(4.8), where the coefficients $a_{i,\beta}(z)$ are supposed to provide a solution $C_\beta(z) = \sum_{i=0}^{2^{\alpha+2}-1} a_{i,\beta}(z)\Phi^i(z)$ to (5.1) modulo 2^β. This Ansatz, substituted in (5.1), produces the congruence

$$zC_\beta^2(z) - C_\beta(z) + 2^\beta \sum_{i=0}^{2^{\alpha+2}-1} b_{i,\beta+1}(z)\Phi^i(z) + 1 = 0 \quad \text{modulo } 2^{\beta+1}.$$

By our assumption on $C_\beta(z)$, we may divide by 2^β. Comparison of powers of $\Phi(z)$ then yields a system of congruences of the form

$$b_{i,\beta+1}(z) + \mathrm{Pol}_i(z) = 0 \quad \text{modulo } 2, \qquad i = 0, 1, \ldots, 2^{\alpha+2} - 1,$$

where $\mathrm{Pol}_i(z)$, $i = 0, 1, \ldots, 2^{\alpha+2} - 1$, are certain Laurent polynomials with integer coefficients. This system being trivially uniquely solvable, we have proved that, for an arbitrary positive integer α, the algorithm of Section 4 will produce a solution $C_{3\cdot 2^\alpha}(z)$ to (5.1) modulo $2^{3\cdot 2^\alpha}$ which is a polynomial in $\Phi(z)$ with coefficients that are Laurent polynomials in z. □

For example, our computer program needs only about 30 seconds to come up with the corresponding congruence modulo $2^{3\cdot 2^2} = 4096$.

Theorem 14. *Let* $\Phi(z) = \sum_{n\geq 0} z^{2^n}$. *Then we have*

$$\begin{aligned}
\sum_{n=0}^{\infty} \mathrm{Cat}_n\, z^n &= 2048z^{14} + 3072z^{13} + 2048z^{12} + 3584z^{11} + 640z^{10} + 2240z^9 + 32z^8 \\
&\quad + 832z^7 + 2412z^6 + 1042z^5 + 2702z^4 + 53z^3 + 2z^2 + z + 1 \\
&\quad + \big(2048z^{12} + 3840z^{10} + 2112z^8 + 2112z^7 + 552z^6 \\
&\qquad + 3128z^5 + 2512z^4 + 4000z^3 + 3904z^2\big)\,\Phi(z) \\
&\quad + \big(2048z^{13} + 3072z^{11} + 1536z^{10} + 1152z^9 + 1024z^8 + 4000z^7 + 3440z^6 \\
&\qquad + 3788z^5 + 3096z^4 + 3416z^3 + 2368z^2 + 288z\big)\,\Phi^2(z) \\
&\quad + \big(2048z^{11} + 2048z^{10} + 2304z^9 + 512z^8 + 2752z^7 + 3072z^6 + 728z^5 \\
&\qquad + 3528z^4 + 1032z^3 + 3168z^2 + 3456z + 3904\big)\,\Phi^3(z) \\
&\quad + \big(2048z^{12} + 3072z^{11} + 1024z^{10} + 2048z^9 + 1152z^8 + 1728z^7 + 2272z^6 + 2464z^5 \\
&\qquad + 3452z^4 + 3154z^3 + 2136z^2 + 3896z + 1600 + \frac{48}{z}\Big)\,\Phi^4(z) \\
&\quad + \big(2048z^{10} + 2048z^9 + 1792z^8 + 1792z^7 + 1088z^6 + 1536z^5 \\
&\qquad + 1704z^4 + 3648z^3 + 3288z^2 + 200z + 3728 + \frac{2272}{z}\Big)\,\Phi^5(z) \\
&\quad + \big(2048z^{11}1024z^9 + 1536z^8 + 3200z^7 + 2816z^6 + 1312z^5 + 3824z^4 \\
&\qquad + 140z^3 + 592z^2 + 3692z + 488 + \frac{2760}{z}\Big)\,\Phi^6(z) \\
&\quad + \big(2048z^9 + 2304z^7 + 2304z^6 + 3520z^5 + 960z^4 + 2456z^3 \\
&\qquad + 2128z^2 + 2936z + 1784 + \frac{4024}{z}\Big)\,\Phi^7(z) \\
&\quad + \big(2048z^{10} + 1024z^9 + 2048z^8 + 512z^7 + 3968z^6 + 1088z^5 + 1888z^4 \\
&\qquad + 832z^3 + 1444z^2 + 2646z + 3258 + \frac{339}{z}\Big)\,\Phi^8(z) \\
&\quad + \big(2048z^8 + 3328z^6 + 1536z^5 + 3008z^4 \\
&\qquad + 320z^3 + 2168z^2 + 1144z + 3992 + \frac{3152}{z}\Big)\,\Phi^9(z) \\
&\quad + \big(2048z^9 + 3072z^7 + 512z^6 + 1408z^5 + 2560z^4
\end{aligned}$$

$$+3424z^3+3408z^2+1316z+3608+\frac{2380}{z}\Big)\Phi^{10}(z)$$
$$+\big(2048z^7+2048z^6+2816z^5+3072z^4+1856z^3$$
$$+2688z^2+1288z+3880+\frac{3904}{z}\Big)\Phi^{11}(z)$$
$$+\big(2048z^8+1024z^7+3072z^6+2048z^5+1408z^4$$
$$+2624z^3+1440z^2+224z+948+\frac{358}{z}\Big)\Phi^{12}(z)$$
$$+\left(2048z^6+2048z^5+3328z^4+2816z^3+1984z^2+384z+2488+\frac{2384}{z}\right)\Phi^{13}(z)$$
$$+\left(2048z^7+1024z^5+512z^4+2432z^3+1792z^2+3040z+336+\frac{260}{z}\right)\Phi^{14}(z)$$
$$+\left(2048z^5+768z^3+256z^2+64z+2752+\frac{2696}{z}\right)\Phi^{15}(z)$$

modulo 4096. (5.7)

The reader is reminded that coefficient extraction from an expression such as the one on the right-hand side of (5.7) is straightforward, via the algorithm described in Section 3 (see (3.1) and the proof of Lemma 9).

6 A non-example

Consider the equation

$$zF^6(z)-F(z)+1=0, \tag{6.1}$$

which has a unique formal power series solution $F(z)$. We note that the coefficients in the series are special instances of numbers that are now commonly known as *Fuß–Catalan numbers*, which have numerous combinatorial interpretations; cf. [2, pp. 59–60]. It was shown in [27, Eq. (36)] that the coefficient of z^λ in the series $F(z)$ has the same parity as the number of free subgroups of index 14λ in the Hecke group $\mathfrak{H}(7)=C_2*C_7$.

If we try our method from Section 4, then already at the mod-2 level we fail: let $F(z)=a_1(z)\Phi(z)+a_0(z)$ modulo 2, for some Laurent polynomials $a_0(z)$ and $a_1(z)$. Upon substitution in (6.1) and simplification using (cf. Proposition 2)

$$\Phi^2(z)+\Phi(z)+1=0 \text{ modulo } 2,$$

we obtain

$$za_0^6(z)+za_0^4(z)a_1^2(z)+a_0(z)+za_1^6(z)+1$$
$$+\Phi(z)\left(za_0^4(z)a_1^2(z)+za_0^2(z)a_1^4(z)+a_1(z)\right)=0 \quad \text{modulo } 2.$$

or, equivalently,

$$z a_0^6(z) + z a_0^4(z) a_1^2(z) + z a_1^6(z) + a_0(z) + 1 = 0 \quad \text{modulo } 2 \tag{6.2}$$

$$z a_0^4(z) a_1^2(z) + z a_0^2(z) a_1^4(z) + a_1(z) = 0 \quad \text{modulo } 2. \tag{6.3}$$

However, this congruence has no solution in Laurent polynomials $a_0(z)$ and $a_1(z)$. For, the Laurent polynomials $a_0^6(z)$, $a_0^4(z)a_1^2(z)$, $a_1^6(z)$, all of them being squares, contain only even powers of z when the coefficients are reduced modulo 2. Consequently, the term $a_0(z)+1$ on the left-hand side of (6.2) can only contain even powers (modulo 2). In particular, $a_0(z)$ must contain the term 1. If we now suppose that $a_0(z)$ and/or $a_1(z)$ contain negative powers of z, then we obtain a contradiction regardless whether the orders (the minimal e such that z^e appears in a Laurent polynomial) of $a_0(z)$ and $a_1(z)$ are the same or not. This implies that both $a_0(z)$ and $a_1(z)$ are actually polynomials in z, with $a_0(z)$ being of the form $a_0(z) = 1 + \widetilde{a}_0(z)$, where $\widetilde{a}_0(z)$ is a polynomial without constant term. If we now multiply both sides of (6.2) by $a_1^2(z)$ and both sides of (6.3) by $a_0^2(z)$, and subsequently add the two congruences, then we obtain

$$z a_1^8(z) + a_0(z) a_1^2(z) + a_0^2(z) a_1(z) + a_1^2(z) = 0 \quad \text{modulo } 2.$$

Dividing by $a_1(z)$ and replacing $a_0(z)$ by $1 + \widetilde{a}_0(z)$, we obtain the equivalent congruence

$$z a_1^7(z) + \widetilde{a}_0(z) a_1(z) + \widetilde{a}_0^2(z) + 1 = 0 \quad \text{modulo } 2.$$

This congruence has no solution since $\widetilde{a}_0(z)$ has no constant term modulo 2.

In the next theorem, we reveal the deeper reason why our method must fail for $F(z)$. Namely, it shows that exponents e of terms z^e which survive in $F(z)$ after reduction of its coefficients modulo 2 may have an arbitrary number of blocks of consecutive 1's. In contrast, a polynomial in $\Phi(z)$ of degree d with coefficients that are Laurent polynomials in z can only have terms z^e, where e contains at most d blocks of consecutive 1's, apart from a right-most block of bounded length.[4]

Theorem 15. *Let $F(z)$ be the unique formal power series solution to the functional equation* (6.1)*. Then the coefficient of z^n in $F(z)$ is odd if, and only if, the sequence of binary digits of n is built by concatenating (in any order) blocks of* 0011 *and* 01*. In particular, the number of free subgroups of index n in $\mathfrak{H}(7) = C_2 * C_7$ is odd if, and only if, the above condition holds.*

Proof. By replacing $F(z)$ by $1 + G(z)$ in (6.1), we obtain

$$z\,(1 + G(z))^6 - G(z) = 0,$$

or, equivalently,

$$z = \frac{G(z)}{(1 + G(z))^6},$$

[4]The length of this right-most block is in fact bounded by the maximal modulus of an exponent of z occurring in a Laurent polynomial coefficient.

so that $G(z)$ is the compositional inverse of the series $z/(1+z)^6$. By the Lagrange inversion formula (cf. [32, Theorem 5.4.2 with $k=1$]), we obtain for $n \geq 1$ that

$$\begin{aligned}\langle z^n \rangle F(z) = \langle z^n \rangle G(z) &= \frac{1}{n} \left\langle z^{-1} \right\rangle \frac{(1+z)^{6n}}{z^n} \\ &= \frac{1}{n} \left\langle z^{n-1} \right\rangle (1+z)^{6n} = \frac{1}{n} \binom{6n}{n-1} = \frac{1}{6n+1} \binom{6n+1}{n}.\end{aligned}$$

By the well-known theorem of Legendre [21, p. 10] (cf. (2.10)), we see that the coefficient of z^n in $F(z)$ is odd if, and only if,

$$s(6n+1) - s(5n+1) - s(n) = 0, \tag{6.4}$$

where, as in Section 2, $s(m)$ denotes the binary digit sum of m. Another way to phrase (6.4) is to say that, whenever we find a 1 in the binary expansion of n, then there must also be a 1 in the binary expansion of $6n+1$ at the same digit place.

We are now ready to establish the claim of the theorem. In view of the above considerations, it suffices to show that the condition on n in the statement of the theorem is equivalent to (6.4).

Let n be a positive integer with the property that its binary expansion is formed by concatenating blocks of the form 0011 and 01. We prove that (6.4) holds in this case by induction on n. It is routine to check that our assertion holds true for $n = 1, 2, \ldots, 15$. Now, let $n = 4n_1 + 1$, with some positive integer n_1. In other words, the right-most digits in the binary expansion of n are 01 and the binary expansion of n_1 is formed by concatenating blocks of the form 0011 and 01. In that case, we have

$$\begin{aligned}&s(6n+1) - s(5n+1) - s(n) \\ &\qquad = s\left(4(6n_1+1)+2+1\right) - s\left(4(5n_1+1)+2\right) - s(4n_1+1) \\ &\qquad = s(6n_1+1) + 2 - s(5n_1+1) - 1 - s(n_1) - 1 = 0,\end{aligned} \tag{6.5}$$

by the induction hypothesis applied to n_1. On the other hand, if $n = 16n_1 + 3$ for some positive integer n_1, that is, if the right-most digits in the binary expansion of n are 0011 and the binary expansion of n_1 is formed by concatenating blocks of the form 0011 and 01, then

$$\begin{aligned}&s(6n+1) - s(5n+1) - s(n) \\ &\qquad = s\left(16(6n_1+1)+2+1\right) - s\left(16(5n_1+1)\right) - s(16n_1+2+1) \\ &\qquad = s(6n_1+1) + 2 - s(5n_1+1) - s(n_1) - 2 = 0,\end{aligned} \tag{6.6}$$

establishing again the truth of (6.4).

In order to prove the converse, let us suppose that n satisfies (6.4). We start by showing that the binary expansion of n cannot contain any of the substrings 111, 000, 1011. We call an occurrence of any of these substrings a "violation."

Assuming that the right-most violation is a substring of the form 111, we have

$$\begin{aligned} n &= \quad \ldots \mathbf{1}110\ldots, \\ 2n &= \quad \ldots 1110\ldots 0, \\ 4n &= \ldots 1110\ldots 00, \\ 6n+1 &= \quad \ldots 1\mathbf{0}1 \quad \ldots 1, \end{aligned}$$

since to the right of the substring 111 in n there are only blocks of the form 0011 and 01 according to our assumption, which implies that there cannot be any carries "destroying" the substring 101 in $6n+1$. However, this means that at the place where we find the bold-face 1 in (the binary expansion of) n we find a 0 in (the binary expansion of) $6n+1$, a contradiction to (6.4).

Now we assume that the right-most violation is a substring of the form 000. In that case, we have

$$\begin{aligned} n &= \quad \ldots \mathbf{1}000\ldots, \\ 2n &= \quad \ldots 1000\ldots 0, \\ 4n &= \ldots 1000\ldots 00, \\ 6n+1 &= \quad \ldots 1\mathbf{0} \quad \ldots 1, \end{aligned}$$

a contradiction to (6.4) for the same reason.

Finally we assume that the right-most violation is a substring of the form 1011. Then we have

$$\begin{aligned} n &= \quad \ldots \mathbf{1}0110\ldots, \\ 2n &= \quad \ldots 10110\ldots 0, \\ 4n &= \ldots 10110\ldots 00, \\ 6n+1 &= \quad \ldots 0\mathbf{0}01 \quad \ldots 1, \end{aligned}$$

since to the right of the substring 1011 in n there are only blocks of the form 0011 and 01 according to our assumption, which implies that there cannot be any carries "destroying" the substring 0001 in $6n+1$. However, this means that at the place where we find the bold-face 1 in n we find a 0 in $6n+1$, again a contradiction to (6.4).

Now let us suppose that $n = 2^\alpha n_1 + n_0$, where n_0 is an α-digit (binary) number formed by concatenating blocks of the form 0011 and 01. By applying the computations (6.5) and (6.6) (possibly several times), one sees that n satisfies (6.4) if, and only if, n_1 does.

We claim that n_1 cannot be even. For, if it were, say $n_1 = 2^\beta n_2$, then n_1 has a 1 at the digit place β while $6n_1+1$ has not, a contradiction to (6.4). But then the already established fact that n, and hence n_1, cannot contain any of the substrings 111, 000, 1011 implies that the right-most digits in the binary expansion of n_1 form either a block 01 or a block 0011. This provides an inductive argument that the binary expansion of n is formed by concatenating blocks of the form 0011 and 01, and thus completes the proof of the theorem. □

7 Free subgroups in lifts of Hecke groups

For integers m, q with $m \geq 1$, $q \geq 3$, and q prime, we consider the group $\Gamma_m(q)$ as defined in (1.3). Denote by $f_\lambda^{(q)}(m)$ the number of free subgroups of index $2qm\lambda$ in $\Gamma_m(q)$. The purpose of this section is to estimate the 2-adic valuation of $f_\lambda^{(q)}(m)$ in the case when q is a Fermat prime. This estimate is based on a recurrence relation for these numbers, which, in turn, results from a specialisation of a differential equation in [27, Sec. 2]. Moreover, this differential equation for the generating function of free subgroup numbers in $\Gamma_m(q)$ will become of crucial importance in Sections 8 and 13.

In order to present the aforementioned differential equation, we first need to compute several important invariants of $\Gamma_m(q)$. Using notation and definitions from [27, Sec. 2], we have $m_{\Gamma_m(q)} = 2qm$, $\chi(\Gamma_m(q)) = -\frac{q-2}{2qm}$, and thus,

$$\mu(\Gamma_m(q)) = 1 - m_{\Gamma_m(q)}\chi(\Gamma_m(q)) = q - 1 = \mu(\mathfrak{H}(q)).$$

Moreover, for the family of zeta-invariants $\{\zeta_\kappa(\Gamma_m(q)) : \kappa \mid 2qm\}$ of $\Gamma_m(q)$, we find that

$$\zeta_\kappa(\Gamma_m(q)) = \begin{cases} 1, & \kappa = m, \\ -1, & \kappa = 2qm, \\ 0, & \text{otherwise.} \end{cases} \tag{7.1}$$

Our first result in this section compares the A-invariants of $\Gamma_m(q)$, as defined in [27, Eq. (14)], to those of the underlying Hecke group $\mathfrak{H}(q)$, and provides an estimate for their 2-adic valuation.

Lemma 16. *(i) For an integer $m \geq 1$ and a prime $q \geq 3$, we have*

$$A_\mu(\Gamma_m(q)) = m^{q-1}A_\mu(\mathfrak{H}(q)), \quad 0 \leq \mu \leq q-1.$$

(ii) We have

$$v_2(A_\mu(\mathfrak{H}(q)) \geq \mu, \quad 0 \leq \mu \leq q-1.$$

Proof. (i) In view of (7.1), we have, for $0 \leq \mu \leq q-1$, that

$$\begin{aligned} A_\mu(\Gamma_m(q)) &= \frac{1}{\mu!}\sum_{j=0}^{\mu}(-1)^{\mu-j}\binom{\mu}{j}2qm(j+1)\left(\prod_{\substack{1\leq k\leq 2qm\\(k,2qm)=m}}(2qmj+k)\right)\big(2qm(j+1)\big)^{-1} \\ &= \frac{1}{\mu!}\sum_{j=0}^{\mu}(-1)^{\mu-j}\binom{\mu}{j}\prod_{\substack{1\leq k\leq 2qm\\(k,2qm)=m}}(2qmj+k) \\ &= \frac{1}{\mu!}\sum_{j=0}^{\mu}(-1)^{\mu-j}\binom{\mu}{j}\prod_{\substack{1\leq k'\leq 2q\\(k',2q)=1}}\big[m(2qj+k')\big] \end{aligned}$$

$$= m^{\varphi(2q)} \frac{1}{\mu!} \sum_{j=0}^{\mu} (-1)^{\mu-j} \binom{\mu}{j} \prod_{\substack{1 \le k' \le 2q \\ (k',2q)=1}} (2qj + k')$$

$$= m^{q-1} A_\mu(\mathfrak{H}(q)),$$

as claimed.

(ii) This follows from [27, Lemma 1]. □

Our next result is a recurrence relation for the subgroup numbers $f_\lambda^{(q)}(m)$.

Lemma 17. *For m, q as in Lemma 16 and $\lambda \ge 1$, we have*

$$f_{\lambda+1}^{(q)}(m) = \sum_{\mu=1}^{q-1} \sum_{\nu=1}^{\mu} \sum_{\substack{\mu_1,\ldots,\mu_\nu>0 \\ \mu_1+\cdots+\mu_\nu=\mu}} \sum_{\substack{\lambda_1,\ldots,\lambda_\nu \ge 0 \\ \lambda_1+\cdots+\lambda_\nu=\lambda-\mu}} \binom{\mu}{\mu_1,\ldots,\mu_\nu} \left(\nu!\,(2q)^\nu\right)^{-1} m^{q-\nu-1} A_\mu(\mathfrak{H}(q))$$
$$\times \prod_{j=1}^{\nu} \left[(\mu_j - 1)! \binom{\lambda_j + \mu_j - 1}{\mu_j - 1} \right] \prod_{j=1}^{\nu} f_{\lambda_j+\mu_j}^{(q)}(m), \quad (7.2)$$

with initial value $f_1^{(q)}(m) = m^{q-1} A_0(\mathfrak{H}(q))$.

Proof. Setting $\mathfrak{G} = \Gamma_m(q)$ in [27, Eq. (18)], and using Part (i) of Lemma 16 to compute $A_\mu(\Gamma_m(q))$ in terms of $A_\mu(\mathfrak{H}(q))$, leads to the differential equation

$$G_m(q;z) = m^{q-1} A_0(\mathfrak{H}(q))$$
$$+ \sum_{\mu=1}^{q-1} \sum_{\nu=1}^{\mu} \sum_{\substack{\mu_1,\ldots,\mu_\nu>0 \\ \mu_1+\cdots+\mu_\nu=\mu}} \binom{\mu}{\mu_1,\ldots,\mu_\nu} \left(\nu!\,(2q)^\nu\right)^{-1} m^{q-\nu-1} A_\mu(\mathfrak{H}(q)) z^\mu \prod_{j=1}^{\nu} \left(G_m(q;z)\right)^{(\mu_j-1)} \quad (7.3)$$

for the generating function $G_m(q;z) := \sum_{\lambda \ge 0} f_{\lambda+1}^{(q)}(m) z^\lambda$. Comparing the coefficient of z^λ in (7.3) for $\lambda \ge 1$ yields (7.2); while, for $\lambda = 0$, we obtain the required initial value $f_1^{(q)}(m)$. □

Given these preparations, we can now show the following estimate for the 2-adic valuation of $f_\lambda^{(q)}(m)$ in the case when q is a Fermat prime.

Proposition 18. (i) *Let $m \ge 1$ be an integer, and let $q \ge 3$ be a Fermat prime. Then we have*

$$v_2(f_\lambda^{(q)}(m)) \ge v_2(m)(\lambda + q - 2), \quad \lambda \ge 1. \quad (7.4)$$

In particular, if m is even, then $f_\lambda^{(q)}(m)$ is zero modulo any given 2-power for all sufficiently large values of λ.

(ii) *For $q = 3$, equality occurs in Inequality (7.4) if, and only if, $\lambda + 1$ is a 2-power.*

Proof. (i) Since (7.4) is trivially true for m odd, we may suppose that $v_2(m) > 0$. We use induction on λ. For $\lambda = 1$, we have

$$v_2(f_1^{(q)}(m)) = v_2(m^{q-1}A_0(\mathfrak{H}(q))) \geq (q-1)v_2(m) = (\lambda + q - 2)v_2(m),$$

as desired. Now suppose that our claim (7.4) holds for all $f_\gamma^{(q)}(m)$ such that $\gamma < L$, with some integer $L \geq 2$, and consider an arbitrary summand

$$S = S(\mu, \nu, \mu_1, \ldots, \mu_\nu, \lambda_1, \ldots, \lambda_\nu)$$

in the recurrence relation (7.2) with $\lambda = L - 1$. We find that

$$\begin{aligned}
v_2(S) &\geq v_2\binom{\mu}{\mu_1, \ldots, \mu_\nu} - v_2(\nu!) - \nu + (q - \nu - 1)v_2(m) \\
&\qquad + v_2(A_\mu(\mathfrak{H}(q))) + \sum_{j=1}^{\nu} v_2(f_{\lambda_j+\mu_j}^{(q)}(m)) \\
&\geq v_2\binom{\mu}{\mu_1, \ldots, \mu_\nu} - v_2(\nu!) - \nu + (q - \nu - 1)v_2(m) + \mu \\
&\qquad + \sum_{j=1}^{\nu} (\lambda_j + \mu_j + q - 2)v_2(m) \\
&\geq v_2\binom{\mu}{\mu_1, \ldots, \mu_\nu} - v_2(\nu!) - \nu + (q - \nu - 1)v_2(m) + \mu \\
&\qquad + (L-1)v_2(m) + (q-2)\nu v_2(m) \\
&\geq (L + q - 2)v_2(m) + (q-3)\nu v_2(m) + v_2\binom{\mu}{\mu_1, \ldots, \mu_\nu} + \mu - \nu - v_2(\nu!),
\end{aligned}$$

where we have used Part (ii) of Lemma 16 plus the induction hypothesis in the second step. Since $\nu \leq \mu$, the desired inequality for the 2-adic valuation of $f_L^{(q)}(m)$ will follow, if we can show that

$$v_2(\nu!) \leq (q-3)\nu v_2(m) + v_2\binom{\mu}{\mu_1, \ldots, \mu_\nu}. \tag{7.5}$$

Since q is a Fermat prime, we have $q - 1 = 2^\alpha$ for some $\alpha \geq 1$. Thus, if $\nu < q - 1$, then, by Legendre's formula for the p-adic valuation of factorials (cf. [21, p. 10]), we get

$$v_2(\nu!) \leq \sum_{i \geq 0} \left\lfloor \frac{2^\alpha - 1}{2^i} \right\rfloor < \sum_{i \geq 1} 2^{\alpha - i} = q - 2,$$

and (7.5) holds, the left-hand side already being compensated by the term

$$(q-3)\nu\, v_2(m) \geq q - 3.$$

On the other hand, for $\nu = q-1$, we have $\mu = \nu = q-1$, $\mu_1 = \cdots = \mu_{q-1} = 1$, $v_2(\nu!) = q-2$, and

$$v_2\binom{\mu}{\mu_1, \ldots, \mu_\nu} = v_2((q-1)!) = q-2,$$

and the desired conclusion holds again. We have thus shown that every summand S on the right-hand side of (7.2) satisfies $v_2(S) \geq (L+q-2)v_2(m)$, which implies that

$$v_2(f_L^{(q)}(m)) \geq (L+q-2)v_2(m),$$

completing the induction.

(ii) For $q = 3$, the recurrence relation (7.2), with λ replaced by $\lambda - 1$, takes the form

$$f_\lambda^{(3)}(m) = 6m\lambda f_{\lambda-1}^{(3)}(m) + \sum_{\substack{\mu,\nu \geq 1 \\ \mu+\nu=\lambda-1}} f_\mu^{(3)}(m) f_\nu^{(3)}(m), \quad \lambda \geq 2, \tag{7.6}$$

with initial value $f_1^{(3)}(m) = 5m^2$. In order to establish our second claim, we rewrite Equation (7.6) as

$$f_\lambda^{(3)}(m) = 6m\lambda f_{\lambda-1}^{(3)}(m) + \begin{cases} 2\sum_{\mu=1}^{\frac{\lambda-2}{2}} f_\mu^{(3)}(m), f_{\lambda-\mu-1}^{(3)}(m), & \lambda \equiv 0 \ (2), \\ 2\sum_{\mu=1}^{\frac{\lambda-3}{2}} f_\mu^{(3)}(m) f_{\lambda-\mu-1}^{(3)}(m) + \left(f_{\frac{\lambda-1}{2}}^{(3)}(m)\right)^2, & \lambda \equiv 1 \ (2), \end{cases}$$

$$\text{for } \lambda \geq 2, \tag{7.7}$$

and argue again by induction on λ. For $\lambda = 1$, Inequality (7.4) is sharp, as required. Now suppose that, for $\lambda < L$ with some $L \geq 2$, Inequality (7.4) with $q = 3$ is sharp if, and only if, $\lambda + 1$ is a 2-power, and consider $f_L^{(3)}(m)$ as given by (7.7). Setting $m = 2^a m'$ with m' odd, we have

$$v_2(6mLf_{L-1}^{(3)}(m)) = 1 + a + v_2(L) + v_2(f_{L-1}^{(3)}(m)) \geq a(L+1) + 1.$$

Consequently, if L is even then, by what we have already shown,

$$v_2(f_L^{(3)}(m)) \geq a(L+1) + 1.$$

For L odd, all terms except possibly $\left(f_{\frac{L-1}{2}}^{(3)}(m)\right)^2$ are divisible by $2^{a(L+1)+1}$ or a higher 2-power, while this exceptional term satisfies

$$v_2\left(f_{\frac{L-1}{2}}^{(3)}(m)\right)^2 \geq a(L+1),$$

with equality occurring (according to our induction hypothesis) if, and only if, $\frac{L-1}{2}+1 = 2^\gamma$ for some $\gamma \geq 1$; that is, if, and only if, $L+1 = 2^{\gamma+1}$ is a 2-power. This completes the induction, and the proof. □

8 Free subgroup numbers for lifts of the inhomogeneous modular group

In this section, we investigate the behaviour of the numbers $f_\lambda^{(3)}(m)$ of free subgroups in lifts of the inhomogeneous modular group $PSL_2(\mathbb{Z}) \cong \mathfrak{H}(3)$ modulo powers of 2. As mentioned in the introduction, the best previous result available in the literature is [29, Theorem 1], which determines the behaviour of $f_\lambda^{(3)}(1)$ modulo 16. The results in this section solve the problem of determining $f_\lambda^{(3)}(m)$ modulo powers of 2 not only for $m = 1$ and the 2-power $2^4 = 16$, but for *all* m and modulo *any* power of 2.

Let $F_m(z) := 1 + \sum_{\lambda \geq 1} f_\lambda^{(3)}(m)\, z^\lambda$ be the generating function for these numbers. (In the notation of the previous section, $F_m(z) = 1 + zG_m(3; z)$.) By specialising $q = 3$ in (7.3), one obtains the differential equation

$$(1 - (6m-2)z)F_m(z) - 6mz^2F_m'(z) - zF_m^2(z) - 1 - (1 - 6m + 5m^2)z = 0. \tag{8.1}$$

Theorem 19. *Let $\Phi(z) = \sum_{n \geq 0} z^{2^n}$, and let α be some positive integer. Then, for every positive integer m, the generating function $F_m(z)$, when reduced modulo $2^{3 \cdot 2^\alpha}$, can be expressed as a polynomial in $\Phi(z)$ of degree at most $2^{\alpha+2} - 1$, with coefficients that are Laurent polynomials in z over the integers.*

Proof. In view of Proposition 18, the assertion is trivially true for even m, the polynomial in $\Phi(z)$ being a polynomial of degree zero in this case. We may thus assume from now on that m is odd.

We apply the method from Section 4. We start by substituting the Ansatz (4.3) in (8.1) and reducing the result modulo 2. In this way, we obtain

$$\sum_{i=0}^{2^{\alpha+2}-1} a_{i,1}(z)\Phi^i(z) + z \sum_{i=0}^{2^{\alpha+2}-1} a_{i,1}^2(z)\Phi^{2i}(z) + 1 = 0 \quad \text{modulo } 2.$$

This congruence is identical with the congruence (5.2). Hence, we can copy the resulting solution from there. Namely, the unique solution to (5.2) (and, hence, to the above congruence) is given by

$$a_{0,1}(z) = \sum_{k=0}^{\alpha} z^{2^k-1} \quad \text{modulo } 2,$$

$$a_{2^{\alpha+1},1}(z) = z^{-1} \quad \text{modulo } 2,$$

with all other $a_{i,1}(z)$ vanishing.

After we have completed the "base step," we now proceed with the iterative steps described in Section 4. We consider the Ansatz (4.6)–(4.8), where the coefficients $a_{i,\beta}(z)$ are supposed to provide a solution $F_{m,\beta}(z) = \sum_{i=0}^{2^{\alpha+2}-1} a_{i,\beta}(z)\Phi^i(z)$ to (8.1) modulo 2^β.

This Ansatz, substituted in (8.1), produces the congruence

$$2^\beta \sum_{i=0}^{2^{\alpha+2}-1} b_{i,\beta+1}(z)\Phi^i(z) + (1-(6m-2)z)F_{m,\beta}(z) \\ - 6mz^2F'_{m,\beta}(z) - zF^2_{m,\beta}(z) - 1 - (1-6m+5m^2)z = 0 \qquad \text{modulo } 2^{\beta+1}.$$

By our assumption on $F_{m,\beta}(z)$, we may divide by 2^β. Comparison of powers of $\Phi(z)$ then yields a system of congruences of the form

$$b_{i,\beta+1}(z) + \mathrm{Pol}_i(z) = 0 \quad \text{modulo } 2, \qquad i = 0, 1, \dots, 2^{\alpha+2}-1,$$

where $\mathrm{Pol}_i(z)$, $i = 0, 1, \dots, 2^{\alpha+2}-1$, are certain Laurent polynomials with integer coefficients. This system being trivially (uniquely) solvable, we have proved that, for an arbitrary positive integer α, the algorithm of Section 4 will produce a solution $F_{m,2^{3\cdot 2^\alpha}}(z)$ to (8.1) modulo $2^{3\cdot 2^\alpha}$ which is a polynomial in $\Phi(z)$ with coefficients that are Laurent polynomials in z. □

We have implemented this algorithm. As an illustration, the next theorem contains the result for the modulus 64.[5]

Theorem 20. *Let $\Phi(z) = \sum_{n\ge 0} z^{2^n}$. Then, for all positive odd integers m, we have*

$$1 + \sum_{\lambda\ge 1} f^{(3)}_\lambda(m)\, z^\lambda = 32z^9 + 48z^7 + 32z^6 + (16m+8)z^5 + (16m+8)z^4 \\ + \left(2m^2+34\right)z^3 + \left(4m^2-4m+24\right)z^2 + \left(5m^2+12\right)z + 1 \\ + \left(48z^4 + 24z^3 + 12z^2 + 60z + 40\right)\Phi(z) \\ + \left(16z^5 + (16m+32)z^4 + (4m^2-32m+68)z^3 + 36z^2 + 22z + 12 + \frac{12}{z}\right)\Phi^2(z) \\ + \left(32z^5 + 32z^4 + (16m-16)z^3 + 40z^2 + 4z + 52 + \frac{28}{z}\right)\Phi^3(z) \\ + \Bigg(32z^7 + 32z^5 + 32z^4 + (16m+24)z^3 + (16m+40)z^2 \\ + (2m^2+16m+38)z + 24 + \frac{35}{z}\Bigg)\Phi^4(z) \\ + \left(32z^3 + 16z^2 + (16m-8)z + 44\right)\Phi^5(z) \\ + \left(16z^3 + 16mz^2 + \left(4m^2-16m+20\right)z + 44 + \frac{50}{z}\right)\Phi^6(z)$$

[5]To be precise, our implementation finds an expression for each fixed m. These particular results can then be put together "manually" into the uniform expression displayed in (8.2).

$$+\left(32z^3+32z^2+(16m+16)z+40+\frac{4}{z}\right)\Phi^7(z) \qquad \text{modulo } 64. \quad (8.2)$$

9 Subgroup numbers for the inhomogeneous modular group

For a finitely generated group Γ, let $s_n(\Gamma)$ denote the number of subgroups of index n in Γ, and write $S_\Gamma(z)$ for the (shifted) generating function $\sum_{n\geq 0} s_{n+1}(\Gamma)\, z^n$.

In this section, we focus on the sequence $\big(s_n(PSL_2(\mathbb{Z}))\big)_{n\geq 1}$ and its generating function $S(z) := S_{PSL_2(\mathbb{Z})}(z)$. We shall show that our method solves the problem of determining these subgroup numbers modulo any given power of 2, thus refining the parity result of Stothers [34] and the mod-8 result from [29, Theorem 2] mentioned in the introduction.

By the first displayed equation on top of p. 276 in [14] (cf. also [20, Eq. (5.29)] with $H=\{1\}$ and $a=b=h=1$), the series $S(z)$ obeys the differential equation

$$(-1+4z^3+2z^4+4z^6-2z^7-4z^9)S(z)+(z^7-z^{10})(S'(z)+S^2(z)) \\ +1+z+4z^2+4z^3-z^4+4z^5-2z^6-2z^8=0. \quad (9.1)$$

The differential equation (9.1) has a unique solution since comparison of coefficients of z^N fixes the initial values, and yields a recurrence for the sequence $\big(s_n(PSL_2(\mathbb{Z}))\big)_{n\geq 1}$ which computes $s_{n+1}(PSL_2(\mathbb{Z}))$ from terms involving only $s_i(PSL_2(\mathbb{Z}))$ with $i\leq n$.

Theorem 21. *Let $\Phi(z)=\sum_{n\geq 0} z^{2^n}$, and let α be some positive integer. Then the generating function $S(z)=S_{PSL_2(\mathbb{Z})}(z)$, when reduced modulo $2^{3\cdot 2^\alpha}$, can be expressed as a polynomial in $\Phi(z)$ of degree at most $2^{\alpha+2}-1$ with coefficients that are Laurent polynomials in z over the integers.*

Proof. We apply the method from Section 4. We start by substituting the Ansatz (4.3) in (9.1) and reducing the result modulo 2. In this way, we obtain

$$\sum_{i=0}^{2^{\alpha+2}-1} a_{i,1}(z)\Phi^i(z)+(z^7+z^{10})\Bigg(\sum_{i=0}^{2^{\alpha+2}-1} i a_{i,1}(z)\Phi^{i-1}(z)\Phi'(z)+\sum_{i=0}^{2^{\alpha+2}-1} a'_{i,1}(z)\Phi^i(z) \\ +\sum_{i=0}^{2^{\alpha+2}-1} a^2_{i,1}(z)\Phi^{2i}(z)\Bigg)+1+z+z^4=0 \quad \text{modulo } 2.$$

We may reduce $\Phi^{2i}(z)$ further using Relation (4.5). This leads to

$$\sum_{i=0}^{2^{\alpha+2}-1} a_{i,1}(z)\Phi^i(z) + (z^7+z^{10})\Bigg(\sum_{i=0}^{2^{\alpha+2}-1} i a_{i,1}(z)\Phi^{i-1}(z)\Phi'(z) + \sum_{i=0}^{2^{\alpha+2}-1} a'_{i,1}(z)\Phi^i(z)$$
$$+ \sum_{i=0}^{2^{\alpha+1}-1} \left(a^2_{i,1}(z) + z^{2^{\alpha+1}} a^2_{i+2^{\alpha+1},1}(z)\right)\Phi^{2i}(z) + \sum_{i=0}^{2^{\alpha}-1} z^{2^{\alpha+1}} a^2_{i+3\cdot 2^{\alpha},1}(z)\Phi^{2i}(z)$$
$$+ \sum_{i=0}^{2^{\alpha}-1} \left(a^2_{i+2^{\alpha+1},1}(z) + a^2_{i+3\cdot 2^{\alpha},1}(z)\right)\Phi^{2i+2^{\alpha+1}}(z)\Bigg) + 1 + z + z^4 = 0 \quad \text{modulo 2.} \quad (9.2)$$

In the same way as in the proof of Theorem 19, one sees that all coefficients $a_{i,1}(z)$ vanish modulo 2, except possibly $a_{0,1}(z)$ and $a_{2^{\alpha+1},1}(z)$. The corresponding congruences obtained by extracting coefficients of $\Phi^0(z)$ and $\Phi^{2^{\alpha+1}}(z)$, respectively, in (9.2), are

$$a_{0,1}(z) + (z^7+z^{10})\left(a'_{0,1}(z) + a^2_{0,1}(z) + z^{2^{\alpha+1}} a^2_{2^{\alpha+1},1}(z)\right) + 1 + z + z^4 = 0 \quad \text{modulo 2} \quad (9.3)$$

and

$$a_{2^{\alpha+1},1}(z) + (z^7+z^{10})\left(a'_{2^{\alpha+1},1}(z) + a^2_{2^{\alpha+1},1}(z)\right) = 0 \quad \text{modulo 2.} \quad (9.4)$$

The only solutions to (9.4) are $a_{2^{\alpha+1},1}(z) = 0$ modulo 2, respectively $a_{2^{\alpha+1},1}(z) = z^{-7}+z^{-4}$ modulo 2. The first option is impossible, since there is no Laurent polynomial $a_{0,1}(z)$ solving the equation resulting from (9.3). Thus, we have

$$a_{2^{\alpha+1},1}(z) = z^{-7} + z^{-4} \quad \text{modulo 2.} \quad (9.5)$$

Use of this result in (9.3) yields the congruence

$$a_{0,1}(z) + z^7(1+z^3)\left(a'_{0,1}(z) + a^2_{0,1}(z)\right) + z^{2^{\alpha+1}-7}(1+z^3)^3 + 1 + z + z^4 = 0 \quad \text{modulo 2.} \quad (9.6)$$

for $a_{0,1}(z)$. We let

$$a_{0,1}(z) = \widetilde{a}_{0,1}(z) + z^{-7} + z^{-4} + z^{-3} + (1+z^3)\sum_{k=2}^{\alpha} z^{2^k-7}$$

and substitute this in (9.6). Thereby, we get

$$\widetilde{a}_{0,1}(z) + z^7(1+z^3)\left(\widetilde{a}'_{0,1}(z) + \widetilde{a}^2_{0,1}(z)\right) + z^{-7} + z^{-4} + z^{-3} + (1+z^3)\sum_{k=2}^{\alpha} z^{2^k-7}$$
$$+ z^7(1+z^3)\left(z^{-8} + z^{-4} + \sum_{k=2}^{\alpha} z^{2^k-8} + z^{-14} + z^{-8} + z^{-6} + (1+z^3)^2\sum_{k=2}^{\alpha} z^{2^{k+1}-14}\right)$$
$$+ z^{2^{\alpha+1}-7}(1+z^3)^3 + 1 + z + z^4 = 0 \quad \text{modulo 2,}$$

or, after simplification,

$$\widetilde{a}_{0,1}(z)+z^7(1+z^3)\left(\widetilde{a}'_{0,1}(z)+\widetilde{a}^2_{0,1}(z)\right)=0 \quad \text{modulo } 2.$$

Again, either $\widetilde{a}_{0,1}(z)=0$ modulo 2 or $\widetilde{a}_{0,1}(z)=z^{-7}+z^{-4}$ modulo 2. Here, the second option is impossible, since it would imply that $S(z)$ contains a negative z-power, which is absurd.

In summary, we have found that

$$a_{0,1}(z)=z^{-7}+z^{-4}+z^{-3}+(1+z^3)\sum_{k=2}^{\alpha} z^{2^k-7} \quad \text{modulo } 2,$$

$$a_{2^{\alpha+1},1}(z)=z^{-7}+z^{-4} \quad \text{modulo } 2,$$

with all other $a_{i,1}(z)$ vanishing, forms the unique solution modulo 2 to the system of congruences resulting from (9.2) in Laurent polynomials $a_{i,1}(z)$. It should be noted that all $a_{i,1}(z)$'s, $1\le i\le 2^{2^{\alpha+2}}-1$, are divisible by $1-z^3$ modulo 2, as is $a_{0,1}(z)-1$.

After we have completed the "base step," we now proceed with the iterative steps described in Section 4. The arguments turn out to be slightly more delicate here than in the proof of Theorem 19. To be more precise, when considering the Ansatz (4.6)–(4.8), where, inductively, the coefficients $a_{i,\beta}(z)$ are supposed to provide a solution $S_\beta(z)=\sum_{i=0}^{2^{\alpha+2}-1} a_{i,\beta}(z)\Phi^i(z)$ to (9.1) modulo 2^β, we must also assume that $a_{i,\beta}(z)$, $1\le i\le 2^{2^{\alpha+2}}-1$, and $a_{0,\beta}(z)-1-2z^2$, are all divisible by $1-z^3$. The reader should note that the divisibility assumptions do indeed hold for $\beta=1$, the term $-2z^2$ being negligible, since for $\beta=1$ we are computing modulo $2^\beta=2$.

The above Ansatz, substituted in (9.1), produces the congruence

$$\begin{aligned}
&2^\beta\sum_{i=0}^{2^{\alpha+2}-1} b_{i,\beta+1}(z)\Phi^i(z)\\
&\qquad+2^\beta(z^7-z^{10})\left(\sum_{i=0}^{2^{\alpha+2}-1} i b_{i,\beta+1}(z)\Phi^{i-1}(z)\Phi'(z)+\sum_{i=0}^{2^{\alpha+2}-1} b'_{i,\beta+1}(z)\Phi^i(z)\right)\\
&\qquad\qquad+(-1+4z^3+2z^4+4z^6-2z^7-4z^9)\sum_{i=0}^{2^{\alpha+2}-1} a_{i,\beta}(z)\Phi^i(z)\\
&\qquad+(z^7-z^{10})\left(\sum_{i=0}^{2^{\alpha+2}-1} i a_{i,\beta}(z)\Phi^{i-1}(z)\Phi'(z)\right.\\
&\qquad\qquad\left.+\sum_{i=0}^{2^{\alpha+2}-1} a'_{i,\beta}(z)\Phi^i(z)+\left(\sum_{i=0}^{2^{\alpha+2}-1} a_{i,\beta}(z)\Phi^i(z)\right)^2\right)\\
&\qquad\qquad+1+z+4z^2+4z^3-z^4+4z^5-2z^6-2z^8=0 \quad \text{modulo } 2^{\beta+1}. \qquad (9.7)
\end{aligned}$$

By our inductive construction, we know that the terms contained in lines 3–7 of (9.7) are divisible by 2^β. Hence, if we were to divide by 2^β and compare coefficients of $\Phi^i(z)$, for $i = 0, 1, \ldots, 2^{\alpha+2} - 1$, we would obtain the modular differential equations

$$b_{i,\beta+1}(z) + (z^7 - z^{10})\big(b'_{i,\beta+1}(z) + (i+1)b_{i+1,\beta+1}\Phi'(z)\big) + \mathrm{Pol}_i(z) = 0 \quad \text{modulo } 2,$$
$$i = 0, 1, \ldots, 2^{\alpha+2} - 1, \quad (9.8)$$

where $\mathrm{Pol}_i(z)$, $i = 0, 1, \ldots, 2^{\alpha+2} - 1$, are certain Laurent polynomials with integer coefficients. If i is odd, then the term $(i+1)b_{i+1,\beta+1}$ in (9.8) vanishes modulo 2. Hence, in this case, the differential equation (9.8) is of the form appearing in Lemma 22. The lemma then says that such a differential equation has a solution if, and only if, the Laurent polynomial $\mathrm{Pol}_i(z)$ satisfies the condition given there. We must therefore verify this condition for our Laurent polynomials $\mathrm{Pol}_i(z)$, arising through division of lines 3–7 of (9.7) by 2^β. We shall actually prove (see the following paragraph) that $\mathrm{Pol}_i(z)$ is divisible by $(1-z^3)^2$, for *all* i with $0 \le i \le 2^{\alpha+2} - 1$. For odd i, Corollary 23 thus implies not only unique existence of solutions $b_{i,\beta+1}(z)$ but also divisibility of these solutions by $1 - z^3$. If we now consider Equation (9.8) for even i, that is,

$$b_{i,\beta+1}(z) + (z^7 - z^{10})b'_{i,\beta+1}(z) + z^7(1 - z^3)b_{i+1,\beta+1}\Phi'(z) + \mathrm{Pol}_i(z) = 0 \quad \text{modulo } 2,$$
$$i = 2, 4, \ldots, 2^{\alpha+2} - 2,$$

then we see that divisibility of $b_{i+1,\beta+1}(z)$ by $1 - z^3$ guarantees that we may again apply Corollary 23 to obtain that there is also a unique solution $b_{i,\beta+1}(z)$ for even i, and that this solution is divisible by $1 - z^3$. In summary, we would have proved that, for an arbitrary positive integer α, the algorithm of Section 4 produces a solution $S_{2^{3\cdot 2^\alpha}}(z)$ to (9.1) modulo $2^{3\cdot 2^\alpha}$, which is a polynomial in $\Phi(z)$ with coefficients that are Laurent polynomials in z. This would establish the claim of the theorem.

It remains to prove that lines 3–7 of (9.7) are indeed divisible by $(1 - z^3)^2$. In order to see this conveniently, we write

$$a_{i,\beta}(z) = d_{i,\beta}(z)(1 - z^3) \quad \text{modulo } (1 - z^3)^2, \qquad i = 1, 2, \ldots, 2^{\alpha+2} - 1,$$

and

$$a_{0,\beta}(z) = -1 - 2z^2 + d_{0,\beta}(z)(1 - z^3) \quad \text{modulo } (1 - z^3)^2,$$

where the $d_{i,\beta}(z)$'s are polynomials of the form $p_0 + p_1 z + p_2 z^2$, for some integers p_0, p_1, p_2. (It should be noted that it is at this point where we use our inductive hypothesis on divisibility of the coefficients $a_{i,\beta}(z)$.) Then, reduction of lines 3–7 of (9.7) modulo $(1-z^3)^2$

leads to the remainder

$$(3+2z(1-z^3))\Bigg(-1-2z^2+(1-z^3)\sum_{i=0}^{2^{\alpha+2}-1} d_{i,\beta}(z)\Phi^i(z)\Bigg)$$
$$+z^7(1-z^3)\Bigg(-4z-3z^2\sum_{i=0}^{2^{\alpha+2}-1} d_{i,\beta}(z)\Phi^i(z)+1+4z^2+4z^4\Bigg)$$
$$+3+6z^2+z(1-z^3) \quad \text{modulo } (1-z^3)^2. \quad (9.9)$$

Using the fact that

$$z^7(1-z^3)=z(1-z^3) \quad \text{modulo } (1-z^3)^2$$

and similar reductions modulo $(1-z^3)^2$, one sees that the expression in (9.9) is in fact divisible by $(1-z^3)^2$, as claimed. This completes the proof of the theorem. □

Recall that, given a Laurent polynomial $p(z)$ over the integers, we write $p^{(o)}(z)$ for the odd part $\frac{1}{2}(p(z)-p(-z))$ and $p^{(e)}(z)$ for the even part $\frac{1}{2}(p(z)+p(-z))$ of $p(z)$, respectively.

Lemma 22. *The differential equation*

$$a(z)+(z^7-z^{10})a'(z)+\mathrm{Pol}(z)=0 \quad \text{modulo } 2, \quad (9.10)$$

where $\mathrm{Pol}(z)$ *is a given Laurent polynomial in* z *with integer coefficients, has a solution that is a Laurent polynomial if, and only if,* $\mathrm{Pol}^{(o)}(z)$ *is divisible by* $1+z^6$ (modulo 2)*. In the latter case, the unique solution is given by*

$$a(z)=\mathrm{Pol}^{(e)}(z)+\frac{1+z^9}{1+z^6}\mathrm{Pol}^{(o)}(z)=\mathrm{Pol}^{(e)}(z)+\frac{1+z^3+z^6}{1-z^3}\mathrm{Pol}^{(o)}(z) \quad \text{modulo } 2.$$

Proof. Let $a_0(z)=z^m$. Then it is obvious that

$$a_0(z)+(z^7-z^{10})a_0'(z)=a_0(z) \quad \text{modulo } 2$$

if m is even, and that

$$a_0(z)+(z^7-z^{10})a_0'(z)=(1+z^6)a_0(z)+z^9a_0(z) \quad \text{modulo } 2$$

if m is odd. The assertion of the lemma follows now immediately. □

Corollary 23. *If, in the differential equation* (9.10)*, the Laurent polynomial* $\mathrm{Pol}(z)$ *is divisible by* $(1-z^3)^2$ (modulo 2)*, then the uniquely determined solution* $a(z)$ *is divisible by* $1-z^3$ (modulo 2)*.*

We have implemented the algorithm described in the proof of Theorem 21. As an illustration, we present the result for the modulus 64.

Theorem 24. *Let* $\Phi(z) = \sum_{n\geq 0} z^{2^n}$. *Then we have*

$$\begin{aligned}
&\sum_{n\geq 0} s_{n+1}(PSL_2(\mathbb{Z}))\, z^n \\
&= 32z^{50} + 48z^{44} + 48z^{41} + 32z^{36} + 32z^{35} + 32z^{33} + 48z^{32} + 16z^{28} + 40z^{26} + 16z^{25} \\
&\quad + 32z^{24} + 32z^{23} + 16z^{22} + 16z^{21} + 52z^{20} + 32z^{19} + 40z^{18} + 60z^{17} \\
&\quad + 48z^{16} + 4z^{14} + 32z^{13} + 4z^{12} + 36z^{11} + 16z^{10} + 60z^9 + 2z^8 + 16z^7 + 4z^6 \\
&\quad + 60z^5 + 44z^4 + 16z^3 + 54z^2 + 60z + 32 + \frac{56}{z} + \frac{36}{z^2} + \frac{51}{z^3} + \frac{33}{z^4} + \frac{52}{z^5} + \frac{1}{z^7} \\
&\quad + \Big(32z^{34} + 32z^{26} + 32z^{25} + 32z^{24} + 16z^{22} + 32z^{21} + 32z^{20} + 32z^{17} + 32z^{16} \\
&\quad + 48z^{14} + 16z^{13} + 16z^{12} + 16z^{11} + 32z^{10} + 32z^8 + 48z^7 + 8z^5 + 8z^4 + 48z^3 + 24z + 32 \\
&\quad + \frac{20}{z} + \frac{12}{z^2} + \frac{8}{z^3} + \frac{36}{z^4} + \frac{4}{z^5} + \frac{24}{z^6}\Big)\Phi(z) \\
&\quad + \Big(32z^{34} + 32z^{29} + 32z^{28} + 32z^{26} + 32z^{24} + 32z^{21} + 48z^{19} + 32z^{18} + 48z^{17} + 32z^{14} \\
&\quad + 48z^{13} + 32z^{12} + 56z^{10} + 8z^9 + 16z^8 + 48z^7 + 24z^6 + 56z^5 + 44z^4 + 16z^3 \\
&\quad + 48z^2 + 40z + 44 + \frac{60}{z} + \frac{50}{z^2} + \frac{48}{z^3} + \frac{8}{z^4} + \frac{50}{z^5} + \frac{52}{z^6} + \frac{52}{z^7}\Big)\Phi^2(z) \\
&\quad + \Big(32z^{28} + 32z^{24} + 32z^{21} + 32z^{20} + 32z^{19} + 48z^{16} + 32z^{14} + 32z^{13} + 32z^{12} \\
&\quad + 32z^{11} + 16z^{10} + 48z^9 + 8z^8 + 48z^6 + 56z^4 + 8z^3 + 16z^2 + 48z + 56 + \frac{32}{z} + \frac{20}{z^2} \\
&\quad + \frac{52}{z^3} + \frac{4}{z^4} + \frac{36}{z^5} + \frac{12}{z^6} + \frac{36}{z^7}\Big)\Phi^3(z) \\
&\quad + \Big(32z^{44} + 32z^{41} + 32z^{33} + 32z^{32} + 32z^{31} + 32z^{30} + 32z^{28} + 32z^{27} + 16z^{26} + 32z^{24} \\
&\quad + 32z^{23} + 48z^{22} + 16z^{21} + 40z^{20} + 32z^{19} + 32z^{18} + 24z^{17} + 16z^{16} + 48z^{15} + 32z^{14} \\
&\quad + 16z^{13} + 8z^{12} + 32z^{11} + 56z^{10} + 56z^9 + 44z^8 + 40z^7 + 48z^6 + 16z^5 + 20z^4 + 56z^3 + 30z^2 \\
&\quad + 32z + 28 + \frac{40}{z} + \frac{34}{z^2} + \frac{52}{z^3} + \frac{17}{z^4} + \frac{26}{z^5} + \frac{40}{z^6} + \frac{29}{z^7}\Big)\Phi^4(z) \\
&\quad + \Big(32z^{32} + 32z^{30} + 32z^{26} + 32z^{24} + 32z^{23} + 32z^{22} + 32z^{21} + 48z^{20} + 48z^{18} + 32z^{16} + 48z^{14} \\
&\quad + 32z^{13} + 48z^{12} + 48z^{11} + 32z^8 + 16z^7 + 56z^6 + 48z^5 + 48z^4 + 40z^3 + 16z^2
\end{aligned}$$

$$+ 32z + 56 + \frac{24}{z} + \frac{24}{z^2} + \frac{20}{z^3} + \frac{24}{z^4} + \frac{40}{z^5} + \frac{20}{z^6}\Bigg)\Phi^5(z)$$

$$+ \Bigg(32z^{32} + 32z^{31} + 32z^{30} + 32z^{27} + 32z^{24} + 32z^{23} + 48z^{19} + 16z^{18} + 48z^{17}$$

$$+ 16z^{15} + 48z^{14} + 32z^{12} + 32z^{11} + 56z^8 + 40z^7 + 56z^6 + 16z^5$$

$$+ 8z^4 + 56z^3 + 4z^2 + 56z + 32 + \frac{8}{z} + \frac{52}{z^2} + \frac{60}{z^3} + \frac{30}{z^4} + \frac{20}{z^5} + \frac{20}{z^6} + \frac{14}{z^7}\Bigg)\Phi^6(z)$$

$$+ \Bigg(32z^{30} + 32z^{26} + 32z^{21} + 32z^{20} + 48z^{18} + 32z^{16} + 48z^{14} + 32z^{13} + 48z^{10} + 16z^9 + 8z^6$$

$$+ 32z^5 + 16z^4 + 16z^3 + 8z^2 + 48z + 40 + \frac{48}{z} + \frac{8}{z^2} + \frac{40}{z^3} + \frac{60}{z^4} + \frac{8}{z^5} + \frac{24}{z^6} + \frac{60}{z^7}\Bigg)\Phi^7(z)$$

modulo 64. (9.11)

10 Counting permutation representations of $\Gamma_m(3)$ for m prime

Let m be a prime and, for a finitely generated group Γ, let $h_\Gamma(n) := |\mathrm{Hom}(\Gamma, S_n)|$. We want to determine the function $h_{\Gamma_m(3)}(n)$ counting the permutation representations of degree n of the lift $\Gamma_m(3)$ of the inhomogeneous modular group $PSL_2(\mathbb{Z}) \cong \mathfrak{H}(3)$. Suppose first that $m \geq 5$, and classify the representations $\Gamma_m(3) \to S_n$ by the image $\rho \in S_n$ of the central element $x^2 = y^3$. The permutation ρ must be of the form

$$\rho = \prod_{i=1}^{r} \sigma_i, \quad 0 \leq r \leq \lfloor n/m \rfloor,$$

with pairwise disjoint m-cycles σ_i.

For fixed r, the symmetric group S_n contains exactly

$$\frac{1}{r!}\binom{n}{m, \ldots, m, n-mr}(m-1)!^r = \frac{n!}{r!\,(n-mr)!\,m^r} \tag{10.1}$$

such elements ρ.

Next, given such ρ, the image of the generator x will contain a certain number s of $2m$-cycles in its disjoint cycle decomposition, $0 \leq s \leq \lfloor r/2 \rfloor$, each of which breaks into two m-cycles when squared. Thus, in order to construct a square root of ρ (i.e., a possible image of x), we need to

(i) fix s in the range $0 \leq s \leq \lfloor r/2 \rfloor$,

(ii) select s 2-element subsets from the r m-cycles of ρ, which can be done in

$$\frac{1}{s!}\binom{r}{2s}\binom{2s}{2,\ldots,2} = \frac{r!}{2^s s!\,(r-2s)!}$$

different ways,

(iii) lift each of these s pairs of m-cycles to a $2m$-cycle (whose square is the product of the two given m-cycles), which can be done in m ways,

(iv) compute σ^ω for each of the $r-2s$ remaining m-cycles σ, where ω is the multiplicative inverse of 2 modulo m, and

(v) select a permutation π subject only to the condition that $\pi^2 = 1$ on the $n - mr$ letters not involved in any of the r m-cycles of ρ.

Hence, there are precisely

$$r!\,h_{C_2}(n-mr)\sum_{s=0}^{\lfloor r/2\rfloor}\frac{m^s}{2^s s!\,(r-2s)!} \tag{10.2}$$

distinct square roots for each ρ involving r m-cycles.

Similarly, the number of cubic roots of such ρ is given by

$$r!\,h_{C_3}(n-mr)\sum_{t=0}^{\lfloor r/3\rfloor}\frac{m^{2t}}{3^t t!\,(r-3t)!} \tag{10.3}$$

(classify the cubic roots by the number t of $3m$-cycles, and use the fact that each product of three disjoint m-cycles is the cube of precisely $2m^2$ $3m$-cycles). Multiplying (10.1)–(10.3) and summing over $r = 0, 1, \ldots, \lfloor n/m\rfloor$, we find that

$$h_{\Gamma_m(3)}(n) = n!\sum_{r=0}^{\lfloor n/m\rfloor}\sum_{s=0}^{\lfloor r/2\rfloor}\sum_{t=0}^{\lfloor r/3\rfloor}\frac{r!\,h_{C_2}(n-mr)h_{C_3}(n-mr)}{2^s 3^t m^{r-s-2t} s!\,t!\,(n-mr)!\,(r-2s)!\,(r-3t)!}, \quad m \geq 5. \tag{10.4}$$

The cases where $m = 2, 3$ have to be treated separately. By arguments similar to the ones above, one finds that

$$h_{\Gamma_2(3)}(n) = n!\sum_{r=0}^{\lfloor n/4\rfloor}\sum_{s=0}^{\lfloor 2r/3\rfloor}\frac{(2r)!\,h_{C_2}(n-4r)h_{C_3}(n-4r)}{2^{2(r-s)}3^s r!\,s!\,(n-4r)!\,(2r-3s)!}, \tag{10.5}$$

and that

$$h_{\Gamma_3(3)}(n) = n!\sum_{r=0}^{\lfloor n/9\rfloor}\sum_{s=0}^{\lfloor 3r/2\rfloor}\frac{(3r)!\,h_{C_2}(n-9r)h_{C_3}(n-9r)}{2^s 3^{2r-s} r!\,s!\,(n-9r)!\,(3r-2s)!}. \tag{10.6}$$

Furthermore, it is well-known that, for a prime p,

$$h_{C_p}(n) = \sum_{k=0}^{\lfloor n/p \rfloor} \frac{n!}{p^k\, k!\, (n-pk)!},$$

which allows us to make Formulae (10.4)–(10.6) completely explicit.

11 Subgroup numbers for the homogeneous modular group

In this section we consider the problem of determining the behaviour of the number of index-n-subgroups in the homogeneous modular group $SL_2(\mathbb{Z})$ modulo powers of 2. By a folklore result that goes back at least to Dey [9], these subgroup numbers are in a direct relation to numbers of permutation representations of $SL_2(\mathbb{Z})$. Our starting point is a recurrence with polynomial coefficients for the latter numbers, which is then translated into a Riccati-type differential equation for the generating function $\sum_{n\geq 0} s_{n+1}(SL_2(\mathbb{Z}))\, z^n$ of the subgroup numbers. (Equation (11.5) displays this equation when reduced modulo 16.) Our method from Section 4 is then applied to this differential equation. Direct application already fails for the modulus 8. Interestingly, if we instead apply our method with the minimal polynomial for the modulus 16 given in Proposition 2, then our algorithm produces a result for modulus 8 (see Theorems 26 and 27), but then fails at the level of modulus 16. By the enhancement of the method outlined in Appendix D, we are nevertheless able to treat the subgroup numbers $s_n(SL_2(\mathbb{Z}))$ modulo 16 as well (see Theorem 28). In view of the already substantial computational effort involved in the case of modulus 16, we did not try to push our analysis further to higher powers of 2. In particular, as opposed to the case of the subgroup numbers of $PSL_2(\mathbb{Z})$, it remains unclear whether it is possible to express the generating function $\sum_{n\geq 0} s_{n+1}(SL_2(\mathbb{Z}))\, z^n$, when the coefficients are reduced modulo 2^γ, as a polynomial in $\Phi(z)$ with coefficients that are Laurent polynomials in z over the integers for all $\gamma \geq 1$. We feel, however, that this should be the case; see Conjecture 29.

Let us start with the aforementioned result (cf. [9, Theorem 6.10], see [10, Prop. 1] for a conceptual proof, plus generalisations) relating the numbers of subgroups of a finitely generated group to the numbers of its permutation representations.

Proposition 25. *Let Γ be a finitely generated group. Then we have*

$$\sum_{n=0}^{\infty} |\operatorname{Hom}(\Gamma, S_n)| \frac{z^n}{n!} = \exp\left(\sum_{n=1}^{\infty} s_n(\Gamma) \frac{z^n}{n}\right). \tag{11.1}$$

We take $\Gamma = \Gamma_2(3) = SL_2(\mathbb{Z})$ and combine (11.1) with (10.5), the latter giving an explicit formula for the homomorphism numbers $h_n := |\operatorname{Hom}(SL_2(\mathbb{Z}), S_n)|$. Using the Guessing package [16], we found a recurrence of order 30 for the sequence $(h_n/n!)_{n\geq 0}$, with

coefficients that are polynomials in n over $\mathbb{Z}$. The validity of the recurrence was verified by computing a certificate using Koutschan's *Mathematica* package `HolonomicFunctions` [19].[6] However, this recurrence is not suitable for our purpose, for which we require a recurrence with coefficients that are polynomials in n over $\mathbb{Z}$, and with leading coefficient n. A recurrence of this form, if it exists, must be a left multiple of the recurrence operator corresponding to the minimal order recurrence. The construction of such left multiples is known as *desingularisation*, and algorithms are known for this purpose [1]. This technique can be used to eliminate factors from the leading coefficient of the recurrence (whenever possible), but it cannot be used to ensure that the leading coefficient be a monic polynomial. The recurrence of order 32 mentioned in Footnote 6, with leading coefficient 1, could indeed be used for our purpose, by simply multiplying it by n. However, since this recurrence has high-degree polynomials as coefficients, we preferred to work with a different recurrence with lower degree polynomials as coefficients. The price to pay is that the order of such a recurrence will be higher. So, by an indeterminate Ansatz, we computed a candidate for a recurrence of the desired form of order 50, with polynomial coefficients of degree at most 5.[7] To be precise, it is the uniquely determined recurrence of the form

$$\sum_{k=0}^{50}\left(\sum_{i=0}^{5} a(k,i)n^i\right)\frac{|\operatorname{Hom}(SL_2(\mathbb{Z}),S_{n-k})|}{(n-k)!}=0, \qquad n\geq 50,$$

where

$$\begin{aligned}
a(0,0) &= a(0,2) = a(0,3) = a(0,4) = a(0,5) = 0,\\
a(0,1) &= 1,\\
a(50,5) &= 4732347653660689327793902112942404420129409272526122660074583\backslash\\
&\qquad 9938970872020450106039430400122325 25,\\
a(50,4) &= -8533333705190515850593358965718176129181944910419697590976 79\backslash\\
&\qquad 3078743106989966250706985019403282594096,\\
a(49,5) &= 2507660784286104701612089471873568042396155618028516886767837\backslash\\
&\qquad 5597642482178453084687637361646341 76,\\
a(49,4) &= a(48,5) = a(48,4) = a(47,5) = a(47,4)\\
&\quad = a(46,5) = a(46,4) = a(45,5) = a(45,4) = 0.
\end{aligned}$$

Subsequently, we checked that this recurrence is a left-multiple of the certified recurrence of order 30, thereby establishing validity of this candidate recurrence of order 50. This

[6]The certificate has 4 megabytes, and, to obtain it, required about 30 hours of computation time. The coefficients of this recurrence are polynomials in n of degree 34. Interestingly, there is a recurrence of order 32 with leading coefficient 1. Although we did not try to prove it, it is likely that the recurrence of order 30 is the recurrence of minimal order.

[7]We used the function `LinSolveQ` of the Guessing package [16], which uses modular arithmetic, in order to solve the arising system of linear equations. *Mathematica*'s built-in linear system solver is not capable of solving it on current hardware due to the huge numerators and denominators of rational numbers which arise during the computation.

last recurrence was then converted into a linear differential equation with polynomial coefficients for the series

$$H(z) := \sum_{n=0}^{\infty} h_n \frac{z^n}{n!} = \sum_{n=0}^{\infty} |\operatorname{Hom}(SL_2(\mathbb{Z}), S_n)| \frac{z^n}{n!}.$$

Finally, this last mentioned differential equation can be translated into a Riccati-type differential equation for the generating function

$$S(z) = \sum_{n\geq 0} s_{n+1}(SL_2(\mathbb{Z}))\, z^n \tag{11.2}$$

for the subgroup numbers of $SL_2(\mathbb{Z})$. This is done by differentiating the relation (11.1), with $\Gamma = SL_2(\mathbb{Z})$, several times and by dividing by $H(z)$. This leads to relations of the form

$$\frac{H^{(k)}(z)}{H(z)} = P_k(S(z), S'(z), \dots), \qquad k = 1, 2, \dots, \tag{11.3}$$

where $P_k(S(z), S'(z), \dots)$ is a polynomial in $S(z)$ and its derivatives, which can be determined explicitly using the Faà di Bruno formula for derivatives of composite functions (cf. [6, Sec. 3.4]; but see also [7, 18]). Substituting these relations in the linear differential equation for $H(z)$, one obtains the announced Riccati-type differential equation for $S(z)$. It turns out that this differential equation has integral coefficients, so that it is amenable to our method from Section 4. The differential equation cannot be displayed here since this would require about ten pages. Its reduction modulo 16 is written out in (11.5). Our method from Section 4 with $\alpha = 0$ applied to (11.5) does in fact *not* produce a result modulo $8 = 2^{3\cdot 2^0}$ (it stops at the level of modulus 4). If, however, we use the method from Section 4 with the minimal polynomial for the modulus 16 in place of the one for the modulus 8, then the method goes through up to modulus 8 (but fails for modulus 16). This yields the following theorem. It refines the parity result [20, Eq. (6.3) with $|H| = 1$, $q = 3$, $m = 2$].

Theorem 26. *Let $\Phi(z) = \sum_{n\geq 0} z^{2^n}$. Then we have*

$$\begin{aligned}
&\sum_{n\geq 0} s_{n+1}(SL_2(\mathbb{Z}))\, z^n \\
&\quad = 4z^{20} + 4z^{17} + 4z^{14} + 4z^{12} + 4z^{10} + 4z^9 + 6z^8 + 4z^5 + 6z^4 + 4z^2 + 4z + 6 \\
&\qquad + \frac{7}{z^2} + \frac{3}{z^3} + \frac{6}{z^6} + \frac{6}{z^7} + \frac{4}{z^8} + \frac{1}{z^9} + \frac{3}{z^{11}} + \frac{6}{z^{12}} \\
&\quad + \left(4z^3 + 4z^2 + \frac{4}{z} + \frac{6}{z^3} + \frac{6}{z^4} + \frac{6}{z^6} + \frac{2}{z^7} + \frac{4}{z^8} + \frac{4}{z^9} + \frac{4}{z^{10}} + \frac{6}{z^{12}} + \frac{2}{z^{13}}\right) \Phi(z) \\
&\qquad + \left(4z^8 + 4z^4 + 4z^3 + 6z^2 + 4 + \frac{4}{z} + \frac{6}{z^2} + \frac{2}{z^3} + \frac{5}{z^4} + \frac{2}{z^5}\right.
\end{aligned}$$

$$+\frac{6}{z^6}+\frac{1}{z^7}+\frac{4}{z^8}+\frac{6}{z^9}+\frac{4}{z^{10}}+\frac{6}{z^{11}}+\frac{6}{z^{12}}+\frac{5}{z^{13}}\Bigg)\Phi^2(z)$$
$$+\left(4z^2+\frac{4}{z^2}+\frac{4}{z^3}+\frac{2}{z^4}+\frac{4}{z^5}+\frac{4}{z^6}+\frac{2}{z^7}+\frac{4}{z^9}+\frac{4}{z^{11}}+\frac{4}{z^{12}}+\frac{2}{z^{13}}\right)\Phi^3(z)$$
$$\text{modulo 8.} \quad (11.4)$$

Proof. The Riccati-type differential equation for $S(z)$ (as defined in (11.2)) modulo 16 is[8]

$$p_0(z)+p_1(z)S(z)+p_2(z)S(z)^2+p_3(z)S(z)^3+p_4(z)S(z)^4+p_5(z)S(z)^5+p_6(z)S'(z)$$
$$+p_7(z)S'(z)^2+p_8(z)S(z)S'(z)+p_9(z)S(z)^2S'(z)+p_{10}(z)S(z)^3S'(z)$$
$$+p_{11}(z)S(z)S'(z)^2+p_{12}(z)S''(z)+p_{13}(z)S(z)S''(z)+p_{14}(z)S(z)^2S''(z)$$
$$+p_{15}(z)S'(z)S''(z)+p_{16}(z)S'''(z)+p_{17}(z)S(z)S'''(z)+p_{18}(z)S''''(z)=0$$
$$\text{modulo 16,} \quad (11.5)$$

with coefficients $p_j(z)$, $j=0,1,\ldots,18$ as displayed in Appendix B.

The differential equation (11.5) has a unique solution since comparison of coefficients of z^N fixes the initial values, and yields a recurrence for the sequence $\big(s_n(SL_2(\mathbb{Z}))\big)_{n\geq 1}$ which computes $s_{n+1}(SL_2(\mathbb{Z}))$ from terms involving only $s_i(SL_2(\mathbb{Z}))$ with $i\leq n$.

Now we apply the method from Section 4 with the polynomial

$$(\Phi^2(z)+\Phi(z)+z)(\Phi^4(z)+6\Phi^3(z)+(2z+3)\Phi^2(z)+(2z+6)\Phi(z)+2z+5z^2) \quad (11.6)$$

in place of the polynomial on the left-hand side of (4.4) to the differential equation (11.5) (that is, in view of Proposition 2 we are aiming at determining the subgroup numbers of $s_n(SL_2(\mathbb{Z}))$ modulo 16). This yields the above result by means of a straightforward computer calculation. □

If we want to know explicitly for which n the subgroup number $s_n(SL_2(\mathbb{Z}))$ is congruent to a particular value modulo 8, then we should first apply the algorithm from Section 3 (see (3.1) and the proof of Lemma 9) in order to express powers of $\Phi(z)$ on the right-hand side of (11.4) in terms of the series $H_{a_1,\ldots,a_r}(z)$. (The corresponding expansions are in fact listed in (2.6) and (2.7).) The result is

$$\sum_{n\geq 0} s_{n+1}(SL_2(\mathbb{Z}))\,z^n=\left(\frac{4}{z^4}+\frac{4}{z^7}+\frac{4}{z^{13}}\right)H_3(z)+\left(\frac{4}{z^4}+\frac{4}{z^7}+\frac{4}{z^{13}}\right)H_{1,1,1}(z)$$
$$+\left(4z^2+\frac{4}{z^2}+\frac{4}{z^3}+\frac{6}{z^4}+\frac{4}{z^5}+\frac{4}{z^6}+\frac{6}{z^7}+\frac{4}{z^9}+\frac{4}{z^{11}}+\frac{4}{z^{12}}+\frac{6}{z^{13}}\right)H_{1,1}(z)$$

[8] We display the differential equation modulo 16 in order to prepare for Theorem 28.

$$+\left(4z^4+4z^3+6z^2+4+4z^8+\frac{4}{z}+\frac{6}{z^2}+\frac{6}{z^3}+\frac{5}{z^4}\right.$$
$$\left.+\frac{2}{z^5}+\frac{2}{z^6}+\frac{1}{z^7}+\frac{4}{z^8}+\frac{6}{z^9}+\frac{4}{z^{10}}+\frac{6}{z^{11}}+\frac{2}{z^{12}}+\frac{5}{z^{13}}\right)H_1(z)$$
$$+4z^{20}+4z^{17}+4z^{14}+4z^{12}+4z^{10}+6z^8+2z^4+6z^3+4z^2+2$$
$$+\frac{6}{z}+\frac{1}{z^2}+\frac{2}{z^4}+\frac{6}{z^5}+\frac{7}{z^6}+\frac{2}{z^7}+\frac{2}{z^8}+\frac{5}{z^9}+\frac{6}{z^{10}}+\frac{1}{z^{11}}+\frac{3}{z^{12}} \quad \text{modulo } 8. \tag{11.7}$$

From this expression, it is a routine (albeit tedious) task to extract an explicit description of the behaviour of the subgroup numbers of $SL_2(\mathbb{Z})$ modulo 8. Since the corresponding result can be stated within moderate amount of space, we present it in the next theorem.

Theorem 27. *The subgroup numbers $s_n(SL_2(\mathbb{Z}))$ obey the following congruences modulo 8 :*

(i) $s_n(SL_2(\mathbb{Z})) \equiv 1 \pmod 8$ *if, and only if,* $n = 1, 2, 4, 10,$ *or if* n *is of the form* $2^\sigma - 3$ *for some* $\sigma \geq 4$;

(ii) $s_n(SL_2(\mathbb{Z})) \equiv 2 \pmod 8$ *if, and only if,* $n = 7, 12, 17,$ *or if* n *is of one of the forms*

$$3\cdot 2^\sigma - 3,\ 3\cdot 2^\sigma - 6,\ 3\cdot 2^\sigma - 12, \quad \text{for some } \sigma \geq 4;$$

(iii) $s_n(SL_2(\mathbb{Z})) \equiv 4 \pmod 8$ *if, and only if,* $n = 3, 22, 23, 27, 46, 47, 51,$ *or if* n *is of one of the forms*

$$2^\sigma + 6,\ 2^\sigma + 7,\ 2^\sigma + 11,\ 2^\sigma + 12,\ 2^\sigma + 18,\ 2^\sigma + 21, \quad \text{for some } \sigma \geq 5, \tag{11.8}$$

$$2^\sigma + 2^\tau - 2,\ 2^\sigma + 2^\tau + 1,\ 2^\sigma + 2^\tau + 3,$$
$$\text{for some } \sigma, \tau \text{ with } \sigma \geq 6 \text{ and } 4 \leq \tau \leq \sigma - 1, \tag{11.9}$$

$$2^\sigma + 2^\tau + 2^\nu - 12,\ 2^\sigma + 2^\tau + 2^\nu - 6,\ 2^\sigma + 2^\tau + 2^\nu - 3,$$
$$\text{for some } \sigma, \tau, \nu \text{ with } \sigma \geq 6,\ 5 \leq \nu \leq \sigma - 1, \text{ and } 3 \leq \tau \leq \nu - 1; \tag{11.10}$$

(iv) $s_n(SL_2(\mathbb{Z})) \equiv 5 \pmod 8$ *if, and only if,* $n = 5,$ *or if* n *is of one of the forms*

$$2^\sigma - 6,\ 2^\sigma - 12, \quad \text{for some } \sigma \geq 5;$$

(v) $s_n(SL_2(\mathbb{Z})) \equiv 6 \pmod 8$ *if, and only if,* $n = 6, 11, 14, 18, 19, 21, 33, 34, 35, 37,$ *or if*

n is of one of the forms

$$2^\sigma - 2,\ 2^\sigma - 4, \qquad \text{for some } \sigma \ge 5, \tag{11.11}$$

$$2^\sigma + 1,\ 2^\sigma + 2,\ 2^\sigma + 3,\ 2^\sigma + 4,\ 2^\sigma + 5,\ 2^\sigma + 10,\ 2^\sigma + 13, \quad \text{for some } \sigma \ge 6, \tag{11.12}$$

$$2^\sigma + 2^\tau - 3,\ 2^\sigma + 2^\tau - 6,\ 2^\sigma + 2^\tau - 12, \quad \text{for some } \sigma, \tau \text{ with } \sigma \ge 7 \text{ and } 5 \le \tau \le \sigma - 2; \tag{11.13}$$

(vi) in the cases not covered by items (i)–(v), $s_n(SL_2(\mathbb{Z}))$ *is divisible by* 8; *in particular,* $s_n(SL_2(\mathbb{Z})) \not\equiv 3, 7 \pmod 8$ *for all* n.

As we already said earlier, the method from Section 4 with the polynomial in (11.6) in place of the polynomial on the left-hand side of (4.4) applied to the differential equation (11.5) does not actually produce a result modulo 16 (although this is what it would be designed to). It only produces the result modulo 8 given in Theorem 26 since, at the mod-16-level, the arising system of equations has no polynomial solutions. Nevertheless, by applying the enhanced method from Appendix D to this last system of equations, a solution modulo 16 can still be found, the result being displayed in our next theorem.

Theorem 28. *Let* $\Phi(z) = \sum_{n\ge 0} z^{2^n}$. *Then we have*

$$\begin{aligned}
&\sum_{n\ge 0} s_{n+1}(SL_2(\mathbb{Z}))\, z^n \\
&= 8z^{74} + 8z^{71} + 8z^{68} + 8z^{67} + 8z^{62} + 8z^{61} + 8z^{57} + 8z^{56} + 8z^{54} + 8z^{50} + 8z^{48} + 8z^{47} \\
&\quad + 8z^{45} + 8z^{44} + 8z^{43} + 8z^{42} + 8z^{41} + 8z^{40} + 8z^{38} + 8z^{35} + 8z^{31} + 8z^{26} + 8z^{24} + 8z^{21} \\
&\quad + 12z^{20} + 12z^{17} + 8z^{16} + 8z^{15} + 4z^{14} + 4z^{12} + 12z^9 + 14z^8 + 8z^7 + 12z^6 + 16z^5 \\
&\quad + 12z^4 + 12z^3 + 8z^2 + 8 + \frac{10}{z} + \frac{12}{z^2} + \frac{3}{z^3} + \frac{14}{z^4} + \frac{9}{z^5} + \frac{4}{z^6} + \frac{12}{z^7} + \frac{4}{z^8} + \frac{3}{z^9} + \frac{6}{z^{10}} \\
&\quad + \Bigg(8z^{73} + 8z^{72} + 8z^{71} + 8z^{69} + 8z^{68} + 8z^{67} + 8z^{66} + 8z^{64} + 8z^{63} + 8z^{62} + 8z^{61} \\
&\quad + 8z^{60} + 8z^{59} + 8z^{55} + 8z^{54} + 8z^{49} + 8z^{47} + 8z^{41} + 8z^{38} + 8z^{36} + 8z^{35} + 8z^{32} + 8z^{30} \\
&\quad + 8z^{29} + 8z^{28} + 8z^{27} + 8z^{24} + 8z^{23} + 8z^{21} + 8z^{17} + 8z^{14} + 8z^{13} + 8z^{12} + 8z^9 + 8z^8 \\
&\quad + 8z^7 + 8z^5 + 12z^4 + 8z^3 + 4 + \frac{16}{z} + \frac{6}{z^2} + \frac{12}{z^3} + \frac{8}{z^4} + \frac{6}{z^5} + \frac{4}{z^7} + \frac{4}{z^9} + \frac{8}{z^{10}} + \frac{14}{z^{11}}\Bigg)\Phi(z) \\
&\quad + \Bigg(8z^{72} + 8z^{69} + 8z^{68} + 8z^{66} + 8z^{65} + 8z^{62} + 8z^{61} + 8z^{58} + 8z^{57} + 8z^{56} + 8z^{55} \\
&\quad + 8z^{53} + 8z^{51} + 8z^{50} + 8z^{49} + 8z^{38} + 8z^{37} + 8z^{36} + 8z^{35} + 8z^{28} + 8z^{25} + 8z^{24} + 8z^{22} \\
&\quad + 8z^{18} + 8z^{17} + 8z^{14} + 8z^{11} + 8z^{10} + 8z^8 + 8z^4 + 12z^3 + 8z^2 + 8 + \frac{4}{z} + \frac{8}{z^2} + \frac{10}{z^3}
\end{aligned}$$

$$+\frac{4}{z^4}+\frac{10}{z^6}+\frac{12}{z^8}+\frac{12}{z^{10}}+\frac{8}{z^{11}}+\frac{2}{z^{12}}\Bigg)\Phi^2(z)$$
$$+\Bigg(8z^{72}+8z^{69}+8z^{67}+8z^{66}+8z^{61}+8z^{60}+8z^{56}+8z^{55}+8z^{50}+8z^{47}+8z^{46}$$
$$+8z^{45}+8z^{42}+8z^{40}+8z^{37}+8z^{33}+8z^{32}+8z^{31}+8z^{30}+8z^{28}+8z^{25}+8z^{20}+8z^{19}$$
$$+8z^{17}+8z^{16}+8z^{13}+8z^{12}+8z^{10}+8z^9+8z^8+8z^3+12z^2+8z+\frac{8}{z}+\frac{4}{z^2}+\frac{4}{z^3}+\frac{10}{z^4}$$
$$+\frac{12}{z^5}+\frac{12}{z^6}+\frac{18}{z^7}+\frac{8}{z^8}+\frac{12}{z^9}+\frac{8}{z^{10}}+\frac{4}{z^{11}}+\frac{12}{z^{12}}+\frac{10}{z^{13}}\Bigg)\Phi^3(z)$$
$$+\Bigg(8z^{72}+8z^{71}+8z^{70}+8z^{67}+8z^{65}+8z^{64}+8z^{63}+8z^{60}+8z^{59}+8z^{58}+8z^{57}$$
$$+8z^{56}+8z^{54}+8z^{53}+8z^{51}+8z^{49}+8z^{48}+8z^{45}+8z^{40}+8z^{37}+8z^{36}+8z^{34}+8z^{33}$$
$$+8z^{32}+8z^{30}+8z^{29}+8z^{28}+8z^{25}+8z^{24}+8z^{21}+8z^{18}+8z^{17}+8z^{13}+8z^{11}+8z^9$$
$$+12z^8+8z^7+8z^6+8z^5+12z^4+12z^3+6z^2+8z+12+\frac{4}{z}+\frac{10}{z^2}+\frac{14}{z^3}+\frac{1}{z^4}$$
$$+\frac{14}{z^5}+\frac{10}{z^6}+\frac{5}{z^7}+\frac{12}{z^8}+\frac{14}{z^9}+\frac{12}{z^{10}}+\frac{2}{z^{11}}+\frac{2}{z^{12}}+\frac{1}{z^{13}}\Bigg)\Phi^4(z)$$
$$+\Bigg(8z^{67}+8z^{65}+8z^{63}+8z^{62}+8z^{58}+8z^{57}+8z^{53}+8z^{52}+8z^{50}+8z^{48}$$
$$+8z^{46}+8z^{44}+8z^{43}+8z^{40}+8z^{39}+8z^{37}+8z^{34}+8z^{33}+8z^{28}+8z^{26}$$
$$+8z^{23}+8z^{20}+8z^{17}+8z^{15}+8z^{13}+8z^{11}+8z^9+8z^8+8z^7+8z^5$$
$$+8z^4+4z^2+8z+\frac{4}{z^2}+\frac{8}{z^3}+\frac{14}{z^4}+\frac{12}{z^5}+\frac{14}{z^7}+\frac{4}{z^9}+\frac{4}{z^{11}}+\frac{6}{z^{13}}\Bigg)\Phi^5(z)$$

modulo 16. (11.14)

We did not attempt to push this analysis further to moduli 32, 64, etc., since the computational effort seemed immodest. With the (not very substantial) evidence of Theorems 26 and 28 (but see Remark 32), we still expect the enhanced method to be successful for any given 2-power.

Conjecture 29. *Let $\Phi(z)=\sum_{n\geq 0} z^{2^n}$, and let γ be a positive integer. Then the generating function $\sum_{n\geq 0} s_{n+1}(SL_2(\mathbb{Z}))\, z^n$, reduced modulo 2^γ, can be expressed as a polynomial in $\Phi(z)$ with coefficients that are Laurent polynomials in z over the integers.*

12 Subgroup numbers for the lift $\Gamma_3(3)$

Continuing in the spirit of the previous section, we now consider the number of index-n-subgroups in the lift $\Gamma_3(3)$ (of the Hecke group $\mathfrak{H}(3)\cong PSL_2(\mathbb{Z})$) modulo powers of 2.

We shall see that, again, our method from Section 4 already fails for modulus 8. While this can again be overcome by, instead, designing the computation so that the target is modulus 16, the method then fails at the level of modulus 16. Moreover, for modulus 16, even the enhancement of the method described in Appendix D fails (see Remark 32). This means that a new phenomenon, not covered by our Ansatz, arises in the behaviour of the subgroup numbers at the level of modulus 16. It would be of great interest to find an explicit description of the hidden scheme behind the mod-16 behaviour of the number of subgroups of index n in $\Gamma_3(3)$, and, more generally, of the behaviour modulo *any* power of 2.

We take $\Gamma = \Gamma_3(3)$ in (11.1) and combine the resulting formula with (10.6), the latter giving an explicit formula for the homomorphism numbers $h_n := |\operatorname{Hom}(\Gamma_3(3), S_n)|$. Using the Guessing package [16], we found a recurrence of order 42 for the sequence $(h_n/n!)_{n\geq 0}$, with coefficients that are polynomials in n over $\mathbb{Z}$. The validity of the recurrence was verified by computing a certificate using Koutschan's *Mathematica* package `HolonomicFunctions` [19].[9] However, again, this recurrence is not suitable for our purpose, for which we require a recurrence with coefficients that are polynomials in n over $\mathbb{Z}$, and with leading coefficient n. By an indeterminate Ansatz, we computed a candidate for a recurrence of the desired form of order 60, with polynomial coefficients of degree at most 10.[10] To be precise, it is the uniquely determined recurrence of the form

$$\sum_{k=0}^{60}\Bigg(\sum_{i=0}^{10} b(k,i)n^i\Bigg)\frac{|\operatorname{Hom}(\Gamma_3(3), S_{n-k})|}{(n-k)!} = 0, \qquad n \geq 60,$$

where

$$\begin{aligned}
b(0,0) &= b(0,2) = b(0,3) = b(0,4) = b(0,5)\\
&= b(0,6) = b(0,7) = b(0,8) = b(0,9) = b(0,10) = 0,\\
b(0,1) &= 1,\\
b(60,8) &= 964912434349623817784652622167867606987914843555745684067\backslash\\
&\qquad 685674009906439191802582046649968632709607936344314779\backslash\\
&\qquad 968758285634960942433336146325393115439265829588779380\backslash\\
&\qquad 098878545137387224746425243347371614219124311065920050\backslash\\
&\qquad 229843044101471019648768642986279281308800224594067990\backslash\\
&\qquad 539461032349694733915947489297372243661012,\\
b(60,10) &= b(60,9) = b(60,4)
\end{aligned}$$

[9] The computation took about one week, producing a certificate of 28 megabytes. The coefficients of this recurrence are polynomials in n of degree up to 105. In this case, we were not able to find a recurrence with leading coefficient 1. (It may still exist.) The best that we found in this direction was a recurrence with leading coefficient a 1828-digit number. Again, although we did not try to prove it, it is likely that the recurrence of order 42 is the recurrence of minimal order.

[10] Again, we used the function `LinSolveQ` of the Guessing package [16] in order to solve the arising system of linear equations.

$$
\begin{aligned}
&= b(59,10) = b(59,9) = b(59,8) = b(59,7) = b(59,6) = b(59,5)\\
&= b(59,4) = b(59,3) = b(59,2) = b(59,1) = b(59,0)\\
&= b(58,10) = b(58,9) = b(58,8) = b(58,7) = b(58,6)\\
&= b(58,5) = b(58,4)\\
&= b(57,10) = b(57,9) = b(57,8) = b(57,7) = b(57,6) = b(57,5) = b(57,4)\\
&= b(56,10) = b(56,9) = b(56,8) = b(56,7) = b(56,6) = b(56,5) = b(56,4)\\
&= b(55,10) = b(55,9) = b(55,8) = b(55,7) = b(55,6) = b(55,5) = b(55,4)\\
&= b(54,10) = b(54,9) = b(54,8) = b(54,7) = b(54,6) = b(54,5) = b(54,4)\\
&= b(53,10) = b(53,9) = b(53,8) = b(53,7) = b(53,6) = b(53,5) = b(53,4)\\
&= b(52,10) = b(52,9) = b(52,8)\\
&= b(50,7) = b(50,6)\\
&= b(49,10) = b(49,9) = b(49,8) = b(49,7) = b(49,6) = b(49,5) = b(49,4)\\
&= b(1,7) = 0.
\end{aligned}
$$

Subsequently, we checked that this recurrence is a left-multiple of the certified recurrence of order 42, thereby establishing validity of this candidate recurrence of order 60. This last recurrence was then converted into a linear differential equation with polynomial coefficients for the series

$$H(z) := \sum_{n=0}^{\infty} h_n \frac{z^n}{n!} = \sum_{n=0}^{\infty} |\operatorname{Hom}(\Gamma_3(3), S_n)| \frac{z^n}{n!}.$$

Finally, this last mentioned differential equation can be translated into a Riccati-type differential equation for the generating function

$$S(z) = \sum_{n\geq 0} s_{n+1}(\Gamma_3(3))\, z^n \tag{12.1}$$

for the subgroup numbers of $\Gamma_3(3)$ in the same way as we obtained (11.5) in the previous section. It turns out that this differential equation has integral coefficients, so that it is amenable to our method from Section 4. The differential equation cannot be displayed here since this would require about 100 pages.[11] Its reduction modulo 16 is written out in (12.3). By applying our method from Section 4 with the minimal polynomial for the modulus 16 (!) in place of the polynomial on the left-hand side of (4.4) to (12.3), we obtain the following theorem. It refines the parity result [20, Eq. (6.3) with $|H| = 1$, $q = 3$, $m = 3$].

Theorem 30. *Let* $\Phi(z) = \sum_{n\geq 0} z^{2^n}$. *Then we have*

$$\sum_{n\geq 0} s_{n+1}(\Gamma_3(3))\, z^n$$

[11] The integers appearing as coefficients have up to 320 digits.

$$= 4z^{62} + 4z^{53} + 4z^{44} + 4z^{35} + 6z^{26} + 4z^{20} + 4z^{14} + 4z^{12} + 4z^{11} + 4z^{10}$$
$$+ 4z^9 + 4z^5 + 6z^4 + 4z^3 + 4z^2 + 4z + 6 + \frac{7}{z^2} + \frac{7}{z^3} + \frac{3}{z^5} + \frac{6}{z^6}$$
$$+ \left(4z^3 + 4z^2 + \frac{4}{z} + \frac{6}{z^3} + \frac{6}{z^4} + \frac{6}{z^6} + \frac{2}{z^7}\right)\Phi(z)$$
$$+ \left(4z^8 + 4z^4 + 4z^3 + 6z^2 + 4 + \frac{4}{z} + \frac{6}{z^2} + \frac{2}{z^3} + \frac{5}{z^4} + \frac{6}{z^5} + \frac{6}{z^6} + \frac{5}{z^7}\right)\Phi^2(z)$$
$$+ \left(4z^2 + \frac{4}{z^2} + \frac{4}{z^3} + \frac{2}{z^4} + \frac{4}{z^5} + \frac{4}{z^6} + \frac{2}{z^7}\right)\Phi^3(z) \qquad \text{modulo 8.} \quad (12.2)$$

Proof. The Riccati-type differential equation for $S(z)$ (as defined in (12.1)) modulo 16 is[12]

$$q_0(z) + q_1(z)S(z) + q_2(z)S(z)S'(z) + q_3(z)S(z)S'(z)^2 + q_4(z)S(z)S'(z)^3$$
$$+ q_5(z)S(z)S'(z)^4 + q_6(z)S(z)S''(z) + q_7(z)S(z)S''(z)^2 + q_8(z)S(z)S'''(z)$$
$$+ q_9(z)S(z)S'''(z)^2 + q_{10}(z)S(z)S''''(z) + q_{11}(z)S(z)S'(z)S''(z)$$
$$+ q_{12}(z)S(z)S'(z)S'''(z) + q_{13}(z)S(z)S'(z)^2S'''(z) + q_{14}(z)S(z)^2 + q_{15}(z)S(z)^2S'(z)$$
$$+ q_{16}(z)S(z)^2S'(z)^2 + q_{17}(z)S(z)^2S'(z)^3 + q_{18}(z)S(z)^2S'(z)^4 + q_{19}(z)S(z)^2S''(z)$$
$$+ q_{20}(z)S(z)^2S'''(z) + q_{21}(z)S(z)^2S'''(z)^2 + q_{22}(z)S(z)^2S''''(z) + q_{23}(z)S(z)^2S'(z)S''(z)$$
$$+ q_{24}(z)S(z)^2S'(z)^2S''(z) + q_{25}(z)S(z)^2S'(z)S'''(z) + q_{26}(z)S(z)^2S'(z)^2S'''(z)$$
$$+ q_{27}(z)S(z)^3 + q_{28}(z)S(z)^3S'(z) + q_{29}(z)S(z)^3S'(z)^2 + q_{30}(z)S(z)^3S'(z)^3$$
$$+ q_{31}(z)S(z)^3S''(z) + q_{32}(z)S(z)^3S'''(z) + q_{33}(z)S(z)^3S'(z)S'''(z) + q_{34}(z)S(z)^4$$
$$+ q_{35}(z)S(z)^4S'(z) + q_{36}(z)S(z)^4S'(z)^2 + q_{37}(z)S(z)^4S'(z)^3 + q_{38}(z)S(z)^4S''(z)$$
$$+ q_{39}(z)S(z)^4S'''(z) + q_{40}(z)S(z)^4S'(z)S''(z) + q_{41}(z)S(z)^4S'(z)S'''(z) + q_{42}(z)S(z)^5$$
$$+ q_{43}(z)S(z)^5S'(z) + q_{44}(z)S(z)^5S'(z)^2 + q_{45}(z)S(z)^5S''(z) + q_{46}(z)S(z)^5S'''(z)$$
$$+ q_{47}(z)S(z)^6 + q_{48}(z)S(z)^6S'(z) + q_{49}(z)S(z)^6S'(z)^2 + q_{50}(z)S(z)^6S''(z)$$
$$+ q_{51}(z)S(z)^6S'''(z) + q_{52}(z)S(z)^7 + q_{53}(z)S(z)^7S'(z) + q_{54}(z)S(z)^8 + q_{55}(z)S(z)^8S'(z)$$
$$+ q_{56}(z)S(z)^9 + q_{57}(z)S(z)^{10} + q_{58}(z)S'(z) + q_{59}(z)S'(z)S''(z) + q_{60}(z)S'(z)S'''(z)$$
$$+ q_{61}(z)S'(z)S'''(z)^2 + q_{62}(z)S'(z)S''''(z) + q_{63}(z)S'(z)^2 + q_{64}(z)S'(z)^2S''(z)$$

[12]We display the differential equation modulo 16 in order to prepare for Remark 32.

$$+ q_{65}(z)S'(z)^2S'''(z) + q_{66}(z)S'(z)^3 + q_{67}(z)S'(z)^3S''(z) + q_{68}(z)S'(z)^3S'''(z)$$
$$+ q_{69}(z)S'(z)^4 + q_{70}(z)S'(z)^5 + q_{71}(z)S''(z) + q_{72}(z)S''(z)S'''(z) + q_{73}(z)S''(z)^2$$
$$+ q_{74}(z)S'''(z) + q_{75}(z)S'''(z)^2 + q_{76}(z)S''''(z) + q_{77}(z)S'''''(z) = 0$$

modulo 16, (12.3)

with coefficients $q_j(z)$, $j = 0, 1, \ldots, 77$ as displayed in Appendix C.

The differential equation (12.3) has a unique solution since comparison of coefficients of z^N fixes the initial values, and yields a recurrence for the sequence $\big(s_n(\Gamma_3(3))\big)_{n\geq 1}$ which computes $s_{n+1}(\Gamma_3(3))$ from terms involving only $s_i(\Gamma_3(3))$ with $i \leq n$.

Now we apply the method from Section 4 with the polynomial in (11.6) in place of the polynomial on the left-hand side of (4.4) to the differential equation (12.3). This yields the above result by means of a straightforward computer calculation.[13] □

Also here, if we want to know criteria in terms of n when a subgroup number $s_n(\Gamma_3(3))$ is congruent to a particular value modulo 8, then we must first apply the algorithm from Section 3 to the right-hand side of (12.2). This leads to the identity

$$\sum_{n\geq 0} s_{n+1}(\Gamma_3(3))\, z^n = \left(\frac{4}{z^4} + \frac{4}{z^7}\right) H_3(z) + \left(\frac{4}{z^4} + \frac{4}{z^7}\right) H_{1,1,1}(z)$$
$$+ \left(4z^2 + \frac{4}{z^2} + \frac{4}{z^3} + \frac{6}{z^4} + \frac{4}{z^5} + \frac{4}{z^6} + \frac{6}{z^7}\right) H_{1,1}(z)$$
$$+ \left(4z^8 + 4z^4 + 4z^3 + 6z^2 + 4 + \frac{4}{z} + \frac{6}{z^2} + \frac{6}{z^3} + \frac{5}{z^4} + \frac{6}{z^5} + \frac{2}{z^6} + \frac{5}{z^7}\right) H_1(z)$$
$$+ 4z^{62} + 4z^{53} + 4z^{44} + 4z^{35} + 6z^{26} + 4z^{20} + 4z^{14} + 4z^{12} + 4z^{11} + 4z^{10}$$
$$+ 2z^4 + 2z^3 + 4z^2 + 2 + \frac{6}{z} + \frac{1}{z^2} + \frac{4}{z^3} + \frac{6}{z^4} + \frac{1}{z^5} + \frac{3}{z^6} \quad \text{modulo } 8, \quad (12.4)$$

from which we can extract the following explicit description of the behaviour of the subgroup numbers of $\Gamma_3(3)$ modulo 8.

Theorem 31. *The subgroup numbers $s_n(\Gamma_3(3))$ obey the following congruences modulo 8 :*

(i) $s_n(\Gamma_3(3)) \equiv 1 \pmod 8$ *if, and only if,* $n = 1, 2, 10$, *or if n is of the form $2^\sigma - 3$ for some $\sigma \geq 4$;*

(ii) $s_n(\Gamma_3(3)) \equiv 2 \pmod 8$ *if, and only if,* $n = 7, 9, 17, 18, 27, 42$, *or if n is of one of the forms*

$$3 \cdot 2^\sigma - 3,\ 3 \cdot 2^\sigma - 6, \quad \text{for some } \sigma \geq 5;$$

[13] The calculation being straightforward, it nevertheless required a machine with substantial amount of memory (we had available 32 gigabytes of memory, of which almost 50% were used).

(iii) $s_n(\Gamma_3(3)) \equiv 4 \pmod 8$ *if, and only if,* $n = 3, 12, 22, 23, 36, 38, 39, 43, 46, 49, 50, 51, 53, 54, 63$, *or if* n *is of one of the forms*

$$2^\sigma + 6,\ 2^\sigma + 7,\ 2^\sigma + 11,\ 2^\sigma + 14,\ 2^\sigma + 17,\ 2^\sigma + 18,\ 2^\sigma + 19,\ 2^\sigma + 21, \quad \text{for some } \sigma \geq 6, \tag{12.5}$$

$$2^\sigma + 2^\tau - 2,\ 2^\sigma + 2^\tau + 1,\ 2^\sigma + 2^\tau + 2,\ 2^\sigma + 2^\tau + 3,\ 2^\sigma + 2^\tau + 5,\ 2^\sigma + 2^\tau + 10,$$
$$2^\sigma + 2^\tau + 13, \quad \text{for some } \sigma, \tau \text{ with } \sigma \geq 6 \text{ and } 5 \leq \tau \leq \sigma - 1, \tag{12.6}$$

$$2^\sigma + 2^\tau + 2^\nu - 6,\ 2^\sigma + 2^\tau + 2^\nu - 3, \quad \text{for some } \sigma, \tau, \nu \text{ with } \sigma \geq 7,\ 6 \leq \nu \leq \sigma - 1,\ \text{and } 5 \leq \tau \leq \nu - 1; \tag{12.7}$$

(iv) $s_n(\Gamma_3(3)) \equiv 5 \pmod 8$ *if, and only if,* $n = 5$, *or if* n *is of the form* $2^\sigma - 6$ *for some* $\sigma \geq 5$;

(v) $s_n(\Gamma_3(3)) \equiv 6 \pmod 8$ *if, and only if,* $n = 6, 11$, *or if* n *is of one of the forms*

$$2^\sigma - 2,\ 2^\sigma + 3,\ 2^\sigma + 4, \quad \text{for some } \sigma \geq 4, \tag{12.8}$$

$$2^\sigma + 1,\ 2^\sigma + 2,\ 2^\sigma + 13, \quad \text{for some } \sigma \geq 5, \tag{12.9}$$

$$2^\sigma + 10, \quad \text{for some } \sigma \geq 6, \tag{12.10}$$

$$2^\sigma + 2^\tau - 6,\ 2^\sigma + 2^\tau - 3, \quad \text{for some } \sigma, \tau \text{ with } \sigma \geq 7 \text{ and } 5 \leq \tau \leq \sigma - 2; \tag{12.11}$$

(vi) in the cases not covered by items (i)–(v), $s_n(\Gamma_3(3))$ *is divisible by* 8; *in particular,* $s_n(\Gamma_3(3)) \not\equiv 3, 7 \pmod 8$ *for all* n.

Remark 32. In the application of the method from Section 4 in the proof of Theorem 31, when we arrive at the mod-8-level, we obtain

$$\begin{aligned}\sum_{n\geq 0} s_{n+1}(\Gamma_3(3))\, z^n &= 4z^{62} + 4z^{53} + 4z^{44} + 4z^{35} + 6z^{26} + 4z^{20} \\ &\quad + 4z^{14} + 4z^{12} + 4z^{11} + 4z^9 + 4z^6 + 4z^4 + \frac{2}{z} + \frac{4}{z^2} + \frac{3}{z^3} + \frac{6}{z^4} \\ &\quad + \left(4z^4 + 4 + \frac{6}{z^2} + \frac{4}{z^3} + \frac{6}{z^5}\right)\Phi(z) + \left(4z^3 + \frac{4}{z} + \frac{2}{z^3} + \frac{4}{z^4} + \frac{2}{z^6}\right)\Phi^2(z) \\ &\quad + \left(4z^2 + \frac{4}{z^2} + \frac{4}{z^3} + \frac{2}{z^4} + \frac{4}{z^5} + \frac{4}{z^6} + \frac{2}{z^7}\right)\Phi^3(z) \\ &\quad + \left(4z^8 + 4z^4 + 4z^3 + 6z^2 + 12 + \frac{4}{z} + \frac{2}{z^2} + \frac{6}{z^3} + \frac{1}{z^4} + \frac{2}{z^5} + \frac{2}{z^6} + \frac{1}{z^7}\right)\Phi^4(z) \\ &\quad + \left(4z^2 + \frac{4}{z^2} + \frac{6}{z^4} + \frac{4}{z^5} + \frac{6}{z^7}\right)\Phi^5(z) \quad \text{modulo } 8. \end{aligned} \tag{12.12}$$

However, the system of equations for the next level, the mod-16-level, has no polynomial solutions.[14] Even the enhancement of our method described in Appendix D fails. (There are actually several problems arising. It turns out that, due to the reduction modulo 2, the variables $b_i(z)$ expressed in (D.10) do not solve the system (D.9) unless one puts further restrictions on $a^{(o)}(z), a^{(e)}(z), \ldots, d^{(o)}(z), d^{(e)}(z)$. But even if we ignore that and continue to follow the procedure described in Appendix D, then a contradiction arises at a later point: one of the factors of the polynomial $P(z)$ turns out to be $(1+z)^{10}$, and the congruence (D.11) with $P_j^{m_j}(z) = (1+z)^{10}$ has no solution.) This *proves* that it is impossible to find a polynomial in $\Phi(z)$ with coefficients that are Laurent polynomials in z over the integers which agrees with the generating function for the subgroup numbers of $\Gamma_3(3)$ modulo 16.

13 A variation I: free subgroup numbers for lifts of Hecke groups

In this section, we consider the functional equation

$$z f^{2^h}(z) - f(z) + 1 = 0, \tag{13.1}$$

which generalises the functional equation (5.1) for the generating function of Catalan numbers. It is easy to see that this equation has a unique formal power series solution. The coefficients of this uniquely determined series can be calculated explicitly by means of the Lagrange inversion formula, the result being

$$\langle z^n \rangle\, f(z) = \frac{1}{n}\binom{2^h n}{n-1}, \tag{13.2}$$

but this will not be relevant here.[15] Again, the numbers in (13.2) are special instances of numbers that are now commonly known as *Fuß–Catalan numbers* (cf. the paragraph containing (6.1)).

Our aim is to determine the coefficients of $f(z)$ modulo powers of 2. Our solution of this problem is that, again, the series $f(z)$ can be expressed as a polynomial in a "basic" series. Here, this basic series is

$$\Phi_h(z) = \sum_{n\geq 0} z^{2^{nh}/(2^h-1)}. \tag{13.3}$$

It will turn out (see Corollary 34) that an adaptation of the proof of the theorem below will allow us to treat as well the behaviour, modulo powers of 2, of free subgroup numbers of lifts of Hecke groups $\mathfrak{H}(q)$, with q a Fermat prime.

[14] The corresponding computation took almost 5 hours, using 94% of the 32 gigabytes of memory of the machine on which the computation was performed.

[15] See Footnote 3.

The theorem below, in a certain sense, extends Theorem 13. It does not, however, reduce to it for $h = 1$, due to the choice that, in the proof below, the reductions in our algorithm are based on the polynomial relation (13.7) for the basic series $\Phi_h(z)$, which, for $h = 1$, is "weaker" than the relation (4.4) which is used in the proof of Theorem 13.

Theorem 33. *For a positive integer h, let $\Phi_h(z) = \sum_{n\geq 0} z^{2^{nh}/(2^h-1)}$, and let α be a further positive integer. Then the unique solution $f(z)$ to (13.1), reduced modulo $2^{2^{\alpha h}}$, can be expressed as a polynomial in $\Phi_h(z)$ of degree at most $2^{(\alpha+1)h} - 1$ with coefficients that are Laurent polynomials in $z^{1/(2^h-1)}$ over the integers.*

Proof. For ease of notation, we replace z by z^{2^h-1} in (13.1), thereby obtaining the equation

$$z^{2^h-1}\tilde{f}^{2^h}(z) - \tilde{f}(z) + 1 = 0, \tag{13.4}$$

with $\tilde{f}(z) = f(z^{2^h-1})$. We now have to prove that, modulo $2^{2^{\alpha h}}$, the series $\tilde{f}(z)$ can be expressed as a polynomial in

$$\tilde{\Phi}_h(z) = \sum_{n=0}^{\infty} z^{2^{nh}} \tag{13.5}$$

of degree at most $2^{(\alpha+1)h} - 1$ with coefficients that are Laurent polynomials in z.

It is readily verified that

$$\tilde{\Phi}_h^{2^h}(z) + \tilde{\Phi}_h(z) + z = 0 \quad \text{modulo } 2, \tag{13.6}$$

whence

$$\left(\tilde{\Phi}_h^{2^h}(z) + \tilde{\Phi}_h(z) + z\right)^{2^{\alpha h}} = 0 \quad \text{modulo } 2^{2^{\alpha h}}. \tag{13.7}$$

We modify our Ansatz (4.2) to

$$\tilde{f}(z) = \sum_{i=0}^{2^{(\alpha+1)h}-1} a_i(z)\tilde{\Phi}_h^i(z) \quad \text{modulo } 2^{2^{\alpha h}}, \tag{13.8}$$

where the $a_i(z)$'s are (at this point) undetermined Laurent polynomials in z.

Next, we gradually find approximations $a_{i,\beta}(z)$ to $a_i(z)$ such that (13.4) holds modulo 2^β, for $\beta = 1, 2, \ldots, 2^{\alpha h}$. To start the procedure, we consider the differential equation (13.4) modulo 2, with

$$\tilde{f}(z) = \sum_{i=0}^{2^{(\alpha+1)h}-1} a_{i,1}(z)\tilde{\Phi}_h^i(z) \quad \text{modulo } 2. \tag{13.9}$$

We substitute the Ansatz (13.9) in (13.4), reduce high powers of $\tilde{\Phi}_h(z)$ by using Relation (13.7), reduce the resulting expression modulo 2, thereby taking advantage of the elementary fact that $\tilde{\Phi}_h'(z) = 1$ modulo 2, and we finally see that the left-hand side of (13.4) becomes a polynomial in $\tilde{\Phi}_h(z)$ of degree at most $2^{(\alpha+1)h} - 1$ with coefficients that are Laurent polynomials in z. Now we compare coefficients of powers $\tilde{\Phi}_h^k(z)$,

$k = 0, 1, \dots, 2^{(\alpha+1)h} - 1$. This yields a system of $2^{(\alpha+1)h}$ equations (modulo 2) for the unknown Laurent polynomials $a_{i,1}(z)$, $i = 0, 1, \dots, 2^{(\alpha+1)h} - 1$. Since we have already done similar computations several times before, we content ourselves with stating the result: all Laurent polynomials $a_{i,1}(z)$ must be zero, except for $a_{0,1}(z)$ and $a_{2^{\alpha h},1}(z)$, which are given by

$$\begin{aligned} a_{0,1}(z) &= \sum_{k=0}^{\alpha-1} z^{2^{kh}-1}, \\ a_{2^{\alpha h},1}(z) &= z^{-1}. \end{aligned} \tag{13.10}$$

After we have completed the "base step," we now proceed with the iterative steps described in Section 4. Our Ansatz here (replacing the corresponding one in (4.6)–(4.8)) is

$$\tilde{f}(z) = \sum_{i=0}^{2^{(\alpha+1)h}-1} a_{i,\beta+1}(z)\tilde{\Phi}_h^i(z) \quad \text{modulo } 2^{\beta+1}, \tag{13.11}$$

with

$$a_{i,\beta+1}(z) := a_{i,\beta}(z) + 2^\beta b_{i,\beta+1}(z), \quad i = 0, 1, \dots, 2^{(\alpha+1)h} - 1, \tag{13.12}$$

where the coefficients $a_{i,\beta}(z)$ are supposed to provide a solution

$$\tilde{f}_\beta(z) = \sum_{i=0}^{2^{(\alpha+1)h}-1} a_{i,\beta}(z)\tilde{\Phi}_h^i(z)$$

to (13.4) modulo 2^β. This Ansatz, substituted in (13.4), produces the congruence

$$z^{2^h-1}\tilde{f}_\beta^{2^h}(z) - \tilde{f}_\beta(z) + 2^\beta \sum_{i=0}^{2^{(\alpha+1)h}-1} b_{i,\beta+1}(z)\tilde{\Phi}_h^i(z) + 1 = 0 \quad \text{modulo } 2^{\beta+1}. \tag{13.13}$$

By our assumption on $\tilde{f}_\beta(z)$, we may divide by 2^β. Comparison of powers of $\tilde{\Phi}_h(z)$ then yields a system of congruences of the form

$$b_{i,\beta+1}(z) + \mathrm{Pol}_i(z) = 0 \quad \text{modulo } 2, \qquad i = 0, 1, \dots, 2^{(\alpha+1)h} - 1, \tag{13.14}$$

where $\mathrm{Pol}_i(z)$, $i = 0, 1, \dots, 2^{(\alpha+1)h} - 1$, are certain Laurent polynomials with integer coefficients. This system being trivially uniquely solvable, we have proved that, for an arbitrary positive integer α, the modified algorithm that we have presented here will produce a solution $\tilde{f}_{2^{\alpha h}}(z)$ to (13.4) modulo $2^{2^{\alpha h}}$ which is a polynomial in $\tilde{\Phi}_h(z)$ with coefficients that are Laurent polynomials in z. □

It has been shown in [27] that the parity pattern of free subgroup numbers in Hecke groups $\mathfrak{H}(q)$, q a Fermat prime, coincides with the parity pattern of (special) Fuß–Catalan numbers. More precisely, let $f_\lambda^{(q)}$ denote the number of free subgroups of index $2q\lambda$ in

the Hecke group $\mathfrak{H}(q)$. (For indices not divisible by $2q$, no free subgroups exist in $\mathfrak{H}(q)$.) Then (see [27, Eq. (37)])

$$f_\lambda^{(q)} = \frac{1}{\lambda}\binom{(q-1)\lambda}{\lambda-1} \quad \text{modulo 2.}$$

The reader should keep in mind that $q-1$ is a 2-power. Theorem 33 says that the generating function for the Fuß–Catalan numbers (13.2), when reduced modulo a given power of 2, can be expressed as a polynomial in $\Phi_h(z)$. We are now going to show that the same is true for the generating function for free subgroup numbers in the Hecke group $\mathfrak{H}(q)$, although the equation it satisfies is different from the functional equation (13.1) for the generating function of Fuß–Catalan numbers. In the corollary below, we present actually a more general result: even the generating function for free subgroup numbers of the lift $\Gamma_m(q)$, when reduced modulo a given power of 2, can be expressed as a polynomial in $\Phi_h(z)$ in the case where q is a Fermat prime. In a certain sense, this extends Theorem 19, although it does not reduce to it for $h=1$. Again, the reason lies in the choice that, in the proof below, the reductions in our algorithm are based on the polynomial relation (13.7) for the basic series $\Phi_h(z)$, which, for $h=1$, is "weaker" than the relation (4.4) which is used in the proof of Theorem 19. On the other hand, the corollary does largely extend the parity result [27, Cor. A'].

Corollary 34. *Let $q=2^{2^f}+1$ be a Fermat prime, and let γ be some positive integer. Then, for every positive integer m, the generating function $F_m(q;z)=1+\sum_{\lambda\geq 1} f_\lambda^{(q)}(m)z^\lambda$ of free subgroup numbers of $\Gamma_m(q)$, when reduced modulo 2^γ, can be expressed as a polynomial in $\Phi_{2^f}(z)$ of degree at most $2^{2^f}\gamma-1$ with coefficients that are Laurent polynomials in $z^{1/(q-2)}$, where the series $\Phi_h(z)$ is defined as in* (13.3).

Proof. In view of Proposition 18, the assertion is trivially true for even m, the polynomial in $\Phi_{2^f}(z)$ being a polynomial of degree zero in this case. We may thus assume from now on that m is odd.

Equation (7.3) provides a Riccati-type differential equation for $F_m(q;z) = 1 + zG_m(q;z)$. Moreover, this equation, considered modulo 2, is the same for every odd m. Namely, we have

$$\begin{aligned}\tfrac{1}{z}\big(F_m(q;z)-1\big) = A_0(\mathfrak{H}(q)) + \sum_{\mu=1}^{q-1}\sum_{\nu=1}^{\mu}\sum_{\substack{\mu_1,\dots,\mu_\nu>0\\ \mu_1+\cdots+\mu_\nu=\mu}} \binom{\mu}{\mu_1,\dots,\mu_\nu}\big(\nu!\,(2q)^\nu\big)^{-1} A_\mu(\mathfrak{H}(q))z^\mu \\ \times\prod_{j=1}^{\nu}\Big(\tfrac{1}{z}\big(F_m(q;z)-1\big)\Big)^{(\mu_j-1)} \qquad \text{modulo 2.}\end{aligned}$$

Moreover, it is shown in [27, Prop. 2] that, modulo 2, this differential equation reduces to

$$zF_m^{q-1}(q;z) - F_m(q;z) + 1 = 0 \quad \text{modulo 2.} \tag{13.15}$$

The latter statement means that reduction of coefficients modulo 2 and usage of the simple fact that

$$F_m''(q;z) = 0 \quad \text{modulo } 2 \tag{13.16}$$

leads from the original differential equation (7.3) for $F_m(q;z) = 1 + G_m(q;z)$ to the congruence (13.15). With $q-1$ being a power of 2 by assumption, we observe that, disregarding the restriction to modulus 2, Equation (13.15) is the special case of (13.1) where $h = 2^f$. In particular, if, for the moment, we assume that $\gamma = 2^{\alpha 2^f}$, for some positive integer α, then we see that the base step of the Ansatz outlined (and applied) in the proof of Theorem 33 (with $h = 2^f$) can be successfully performed here: it would yield exactly the same result as there, namely (13.9) with the Laurent polynomials $a_{i,1}(z)$ being given in the paragraph containing (13.10).

However, also the subsequent iterative steps would just work in the same way as in the preceding proof! Indeed, transform the Riccati-type differential equation (7.3) for $F_m(q;z)$ by the substitution $z \mapsto z^{q-2}$ (in analogy with the substitution leading to (13.4)). This yields a Riccati-type differential equation for $F_m(q;z^{q-2})$. A fine point to be observed here is that, in this equation, the coefficients will not necessarily be integral; due to the substitution rule for differentials, denominators that are powers of $(q-2)$ may occur. As in the proof of Theorem 33, we now continue with the Ansatz

$$F_m(q;z^{q-2}) = \sum_{i=0}^{2^{(\alpha+1)2^f}-1} a_{i,\beta+1}(z)\tilde{\Phi}_{2^f}^i(z) \quad \text{modulo } 2^{\beta+1}, \tag{13.17}$$

with

$$a_{i,\beta+1}(z) := a_{i,\beta}(z) + 2^\beta b_{i,\beta+1}(z), \quad i = 0,1,\dots,2^{(\alpha+1)2^f}-1 \tag{13.18}$$

(which is analogous to (13.11)–(13.12)), where the coefficients $a_{i,\beta}(z)$ are supposed to provide a solution

$$F_{m,\beta}(q;z) = \sum_{i=0}^{2^{(\alpha+1)2^f}-1} a_{i,\beta}(z)\tilde{\Phi}_{2^f}^i(z)$$

to the differential equation for $F_m(q;z^{q-2})$ modulo 2^β. The fact that reduction modulo 2 and usage of (13.16) leads from the original differential equation for $F_m(q;z)$ to (13.15) implies that substitution of the Ansatz (13.17)–(13.18) in the differential equation for $F_m(q;z^{q-2})$ yields an equation completely analogous to (13.13), namely

$$z^{q-2}F_{m,\beta}^{q-1}(q;z) - F_{m,\beta}(q;z) + 2^\beta \sum_{i=0}^{2^{\alpha+h}-1} b_{i,\beta+1}(z)\tilde{\Phi}_h^i(z) + 1 + T(z,F_{m,\beta}(q;z)) = 0 \quad \text{modulo } 2^{\beta+1}.$$

Here, $T(z,F_{m,\beta}(q;z))$ consists only of terms that may depend on $F_{m,\beta}(q;z)$ but *do not* depend on the $b_{i,\beta+1}(z)$'s. The rest of the procedure is then as in the preceding proof: we divide by 2^β, compare powers of $\tilde{\Phi}_h(z)$, and obtain a system of congruences of the

form (13.14), which is trivially solvable. The powers of $(q-2)$ that may appear in the denominators of the coefficients in the polynomials involved here are disposed of by interpreting them appropriately as elements of $\mathbb{Z}/2^\gamma\mathbb{Z}$.

Finally, if we are able to express $F_m(q;z)$ as a polynomial in $\Phi_{2^f}(z)$ modulo $2^\gamma = 2^{2^{\alpha 2^f}}$ for all α, then the same assertion must hold for *every* γ. □

In order to illustrate the algorithm described in the last proof, let us consider the case of the Hecke group $\mathfrak{H}(5)$, that is, the case of Corollary 34 where $f=1$. The Riccati-type differential equation for the series $G_m(z) := G_m(5;z) = \sum_{\lambda=0}^\infty f_{\lambda+1}^{(5)}(m)z^\lambda$ that one obtains from (7.3) in this special case reads

$$\begin{aligned}
G_m(z) &= 189m^4 + 4600m^3 z G_m(z) + 1430m^2 z^2 G_m^2(z) + 80mz^3 G_m^3(z) \\
&\quad + z^4 G_m(z)^4 + 14300m^3 z^2 G_m'(z) + 2400m^2 z^3 G_m(z) G_m'(z) + 60mz^4 G_m^2(z) G_m'(z) \\
&\quad + 300m^2 z^4 \big(G_m'(z)\big)^2 + 8000m^3 z^3 G_m''(z) + 400m^2 z^4 G_m(z) G_m''(z) + 1000m^3 z^4 G_m'''(z).
\end{aligned}$$

Since $G_m(z) = G_m(5;z) = \frac{1}{z}\big(F_m(5;z)-1\big)$, we obtain the differential equation

$$\begin{aligned}
&1 + (189m^4 - 300m^3 + 130m^2 - 20m + 1)z \\
&\quad + ((300m^3 - 260m^2 + 60m - 4)z - 1)F_m(5;z) + (130m^2 - 60m + 6)zF_m^2(5;z) \\
&\quad + (20m-4)zF_m^3(5;z) + zF_m^4(5;z) + (4300m^3 - 1000m^2 + 60m)z^2 F_m'(5;z) \\
&+ (1000m^2 - 120m)z^2 F_m(5;z)F_m'(5;z) + 60mz^2 F_m(5;z)^2 F_m'(5;z) + 300m^2 z^3 F_m'(5;z)^2 \\
&\quad + (5000m^3 - 400m^2)z^3 F_m''(5;z) + 400m^2 z^3 F_m(5;z)F_m''(5;z) + 1000m^3 z^4 F_m'''(5;z) = 0
\end{aligned} \tag{13.19}$$

for $F_m(5;z)$. We have implemented the algorithm described in the proof of Theorem 34 for this differential equation. For the modulus 16, it produces the following result. (It is independent of m because of the high divisibility of the coefficients in the differential equation (13.19) by powers of 2. The parameter m will show up for 2-powers higher than $2^4 = 16$.)

Theorem 35. *Let $\Phi_2(z) = \sum_{n\ge 0} z^{4^n/3}$, as before. Then, for all positive odd integers m, the generating function $F_m(5;z) = 1 + \sum_{\lambda\ge 1} f_\lambda^{(5)}(m)z^\lambda$ for the free subgroup numbers of $\Gamma_m(5)$ satisfies*

$$\begin{aligned}
F_m(5;z) &= 4z + 1 + 12z^{2/3}\Phi_2(z) + 10z^{1/3}\Phi_2^2(z) + 12\Phi_2^3(z) + \big(4z^{2/3} + 7z^{-1/3}\big)\Phi_2^4(z) \\
&\quad + 4z^{1/3}\Phi_2^5(z) + 4\Phi_2^6(z) + 12z^{-1/3}\Phi_2^7(z) + 8z^{1/3}\Phi_2^8(z) + 4\Phi_2^9(z) \\
&\quad + 2z^{-1/3}\Phi_2^{10}(z) + 12\Phi_2^{12}(z) + 12z^{-1/3}\Phi_2^{13}(z) \quad \text{modulo } 16.
\end{aligned} \tag{13.20}$$

Clearly, coefficient extraction from powers of $\Phi_2(z)$ (and, more generally, from powers of $\Phi_h(z)$) can be accomplished by appropriately adapting the results in Section 3.

14 A variation II: subgroup numbers for Hecke groups

In Section 9, we proved that the generating function for the subgroup numbers of the inhomogeneous modular group $PSL_2(\mathbb{Z}) \cong \mathfrak{H}(3)$, when reduced modulo a power of 2, can always be expressed as a polynomial in the basic series $\Phi(z)$ with coefficients that are Laurent polynomials in z. Here, we discuss possible extensions of this result to Hecke groups $\mathfrak{H}(q)$, where q is a Fermat prime. Again, we have to modify the original method from Section 4 by using the series $\Phi_h(z)$ defined in (13.3) (for suitable h) instead of $\Phi(z)$. We conjecture (see Conjecture 38) that this variation of our method will be successful for arbitrary Fermat primes q. If $q = 5$, we are actually able to demonstrate this conjecture, thereby largely refining the $q = 5$ case of [27, Theorem B].

Theorem 36. *With notation from the previous section, let $\Phi_2(z) = \sum_{n\geq 0} z^{4^n/3}$, and let α be a positive integer. Then the generating function $S(z) = S_{\mathfrak{H}(5)}(z)$ (see the first paragraph of Section 9 for the definition), reduced modulo 2^{4^α}, can be expressed as a polynomial in $\Phi_2(z)$ of degree at most $4^{\alpha+1} - 1$ with coefficients that are Laurent polynomials in $z^{1/3}$ over the integers.*

Proof. Let

$$h(n) = \frac{1}{n!} h_{C_2}(n) h_{C_5}(n).$$

Using the routine to compute recurrences for the Hadamard product of recursive sequences, implemented in `gfun` [31] and `GeneratingFunctions` [23] (cf. [32, Theorem 6.4.12] for the theoretical background), one obtains the recurrence

$$\begin{aligned}
&n(16 - 72n + 174n^2 - 155n^3 + 65n^4 - 13n^5 + n^6)h(n) \\
&\qquad - (184 - 620n + 854n^2 - 555n^3 + 177n^4 - 25n^5 + n^6)h(n-1) \\
&\qquad - (856 - 1636n + 1250n^2 - 479n^3 + 101n^4 - 13n^5 + n^6)h(n-2) \\
&\qquad - 4(n-6)(n-3)^2(-7+3n)h(n-3) + 8(n-7)(n-4)(3n-7)h(n-4) \\
&- (1136 - 856n + 1292n^2 - 2930n^3 + 3115n^4 - 1718n^5 + 516n^6 - 80n^7 + 5n^8)h(n-5) \\
&- 2(1856 - 5376n + 6828n^2 - 4868n^3 + 2174n^4 - 651n^5 + 133n^6 - 17n^7 + n^8)h(n-6) \\
&-4(n-6)(n-5)(n-3)^2(n-2)(3n-7)h(n-7)+8(n-7)(n-6)(n-4)(n-3)(3n-7)h(n-8) \\
&\qquad - 16(n-8)(n-7)(n-5)(-7+3n)h(n-9) \\
&- (n-9)(n-8)(n-6)(n-3)(16 + 12n - 16n^2 - 5n^3 + 15n^4 - 7n^5 + n^6)h(n-10) = 0
\end{aligned} \tag{14.1}$$

for the sequence $\big(h(n)\big)_{n\geq 0}$. Since the leading coefficient (i.e., the coefficient of $h(n)$) is not n, this recurrence is not suitable for being translated into a Riccati-type differential

equation with integral coefficients via (11.1), to which we can apply our method from Section 4. Using Euclidean division of difference operators, one can see that we also have

$$\begin{aligned}
&nh(n) - h(n-1) - h(n-2) - \left(5n^2 - 11n - 44\right) h(n-5) - 2(n-4)(n-2)h(n-6) \\
&\quad + 12h(n-7) - 4h(n-8) - \left(n^4 - 20n^3 + 95n^2 + 260n - 2000\right) h(n-10) \\
&\quad + 4(9n-85)h(n-11) - 8\left(n^2 - 19n + 89\right) h(n-12) \\
&\quad + 4(n-14)(n-13)(n-11)(n-7)h(n-15) \\
&\quad - 4(n-15)(n-14)(n-12)(n-9)h(n-16) = 0. \quad (14.2)
\end{aligned}$$

If we now apply the procedure of converting such a recurrence for homomorphism numbers (divided by $n!$) into a Riccati-type differential equation for the generating function of the corresponding subgroup numbers as explained in the paragraph containing (11.2), then we obtain the differential equation

$$\begin{aligned}
&224z^{15} - 256z^{14} + 40z^{11} - 56z^{10} + 100z^9 + 4z^7 - 12z^6 + 16z^5 + 26z^4 + z + 1 \\
&\quad + \left(736z^{16} - 824z^{15} + 48z^{12} - 36z^{11} + 276z^{10} + 14z^6 + 44z^5 - 1\right) S(z) \\
&\quad + \left(448z^{17} - 488z^{16} + 8z^{13} + 162z^{11} + 2z^7 + 5z^6\right) S^2(z) \\
&\quad + \left(80z^{18} - 84z^{17} + 26z^{12}\right) S^3(z) + \left(4z^{19} - 4z^{18} + z^{13}\right) S^4(z) \\
&\quad + \left(448z^{17} - 488z^{16} + 8z^{13} + 162z^{11} + 2z^7 + 5z^6\right) S'(z) \\
&\quad + \left(12z^{19} - 12z^{18} + 3z^{13}\right) (S')^2(z) + \left(240z^{18} - 252z^{17} + 78z^{12}\right) S(z)S'(z) \\
&\quad + \left(24z^{19} - 24z^{18} + 6z^{13}\right) S^2(z)S'(z) + \left(80z^{18} - 84z^{17} + 26z^{12}\right) S''(z) \\
&\quad + \left(16z^{19} - 16z^{18} + 4z^{13}\right) S(z)S''(z) + \left(4z^{19} - 4z^{18} + z^{13}\right) S'''(z) = 0. \quad (14.3)
\end{aligned}$$

For convenience, we replace z by z^3 in (14.3). Writing $\tilde{S}(z) = S(z^3)$, the above differential equation translates into

$$\begin{aligned}
&224z^{45} - 256z^{42} + 40z^{33} - 56z^{30} + 100z^{27} + 4z^{21} - 12z^{18} + 16z^{15} + 26z^{12} + z^3 + 1 \\
&\quad + \left(736z^{48} - 824z^{45} + 48z^{36} - 36z^{33} + 276z^{30} + 14z^{18} + 44z^{15} - 1\right) \tilde{S}(z) \\
&\quad + \left(448z^{51} - 488z^{48} + 8z^{39} + 162z^{33} + 2z^{21} + 5z^{18}\right) \tilde{S}^2(z) \\
&\quad + \left(80z^{54} - 84z^{51} + 26z^{36}\right) \tilde{S}^3(z) + \left(4z^{57} - 4z^{54} + z^{39}\right) \tilde{S}^4(z) \\
&\quad - \frac{1}{27} z^{16} \left(96z^{36} - 3688z^{33} + 3928z^{30} - 72z^{21} + 24z^{18} - 1312z^{15} - 18z^3 - 45\right) \tilde{S}'(z) \\
&\quad + \frac{1}{3} z^{35} \left(4z^{18} - 4z^{15} + 1\right) (\tilde{S}')^2(z) + \left(80z^{52} - 84z^{49} + 26z^{34}\right) \tilde{S}(z)\tilde{S}'(z)
\end{aligned}$$

$$+\left(8z^{55}-8z^{52}+2z^{37}\right)\tilde{S}^2(z)\tilde{S}'(z)+\frac{4}{9}z^{32}\left(4z^{21}+14z^{18}-19z^{15}+z^3+6\right)\tilde{S}''(z)$$
$$+\frac{1}{27}z^{33}\left(4z^{18}-4z^{15}+1\right)\tilde{S}'''(z)=0. \quad (14.4)$$

We have to prove that, modulo 2^{4^α}, the series $\tilde{S}(z)$ can be expressed as a polynomial in $\tilde{\Phi}_2(z)$ (as defined in (13.5)) of degree at most $4^{\alpha+1}-1$ with coefficients that are Laurent polynomials in z.

We make the Ansatz

$$\tilde{S}(z)=\sum_{i=0}^{4^{\alpha+1}-1}a_i(z)\tilde{\Phi}_2^i(z) \quad \text{modulo } 2^{4^\alpha}, \quad (14.5)$$

where the $a_i(z)$'s are (at this point) undetermined Laurent polynomials in z.

Next we gradually find approximations $a_{i,\beta}(z)$ to $a_i(z)$ such that (14.4) holds modulo 2^β, for $\beta=1,2,\dots,4^\alpha$. To start the procedure, we consider the differential equation (14.4) modulo 2, with

$$\tilde{S}(z)=\sum_{i=0}^{4^{\alpha+1}-1}a_{i,1}(z)\tilde{\Phi}_2^i(z) \quad \text{modulo } 2. \quad (14.6)$$

We substitute the Ansatz (14.6) in (14.4), reduce high powers of $\tilde{\Phi}_2(z)$ by using the relation (13.7) with $h=2$, and reduce the resulting expression modulo 2, thereby taking advantage of the elementary fact that $\tilde{\Phi}_2'(z)=1$ modulo 2. The powers of 3 that appear in the denominators of the coefficients in the polynomials involved here are disposed of by interpreting them appropriately as elements of $\mathbb{Z}/2^{4^\alpha}\mathbb{Z}$. We finally see that the left-hand side of (14.4) becomes a polynomial in $\tilde{\Phi}_2(z)$ of degree at most $4^{\alpha+1}-1$ with coefficients that are Laurent polynomials in z. Now we compare coefficients of powers $\tilde{\Phi}_2^k(z)$ for $k=0,1,\dots,4^{\alpha+1}-1$. This yields a system of $4^{\alpha+1}$ equations (modulo 2) for the unknown Laurent polynomials $a_{i,1}(z)$, $i=0,1,\dots,4^{\alpha+1}-1$. Since we have already done similar computations several times before, we content ourselves with stating the result: all Laurent polynomials $a_{i,1}(z)$ must be zero, except for

$$a_{0,1}(z)=z^{-9}+z^{-13}\sum_{k=1}^{\alpha-1}z^{4^k}+z^{-8}\sum_{k=1}^{\alpha-1}z^{2\cdot 4^k},$$
$$a_{4^\alpha,1}(z)=z^{-13},$$
$$a_{2\cdot 4^\alpha,1}(z)=z^{-8}. \quad (14.7)$$

After we have completed the "base step," we now proceed with the iterative steps described in Section 4. Our Ansatz here (replacing the corresponding one in (4.6)–(4.8)) is

$$\tilde{S}(z)=\sum_{i=0}^{4^{\alpha+1}-1}a_{i,\beta+1}(z)\tilde{\Phi}_2^i(z) \quad \text{modulo } 2^{\beta+1}, \quad (14.8)$$

with

$$a_{i,\beta+1}(z) := a_{i,\beta}(z) + 2^{\beta} b_{i,\beta+1}(z), \quad i = 0, 1, \dots, 4^{\alpha+1} - 1, \tag{14.9}$$

where the coefficients $a_{i,\beta}(z)$ are supposed to provide a solution

$$\tilde{S}_{\beta}(z) = \sum_{i=0}^{4^{\alpha+1}-1} a_{i,\beta}(z) \tilde{\Phi}_2^i(z)$$

to (14.4) modulo 2^{β}. This Ansatz, substituted in (14.4), produces a congruence of the form

$$T(\tilde{S}_{\beta}(z)) + 2^{\beta} \sum_{i=0}^{4^{\alpha+1}-1} \big(b_{i,\beta+1}(z) + z^{16} b'_{i,\beta+1}(z) + (i+1) b_{i+1,\beta+1}(z)\big) \tilde{\Phi}_2^i(z) + 1 = 0$$

$$\text{modulo } 2^{\beta+1}, \tag{14.10}$$

where $T(\tilde{S}_{\beta}(z))$ represents terms that only depend on $\tilde{S}_{\beta}(z)$. Inductively, we have already computed $\tilde{S}_{\beta}(z)$, and we know that $T(\tilde{S}_{\beta}(z))$ must be divisible by 2^{β}. Comparison of powers of $\tilde{\Phi}_2(z)$ then yields a system of congruences that is equivalent to a system of the form

$$b_{i,\beta+1}(z) + z^{16} b'_{i,\beta+1}(z) + \mathrm{Pol}_i(z) = 0 \quad \text{modulo } 2, \qquad i = 0, 1, \dots, 4^{\alpha+1} - 1,$$

where $\mathrm{Pol}_i(z)$, $i = 0, 1, \dots, 4^{\alpha+1} - 1$, are certain Laurent polynomials with integer coefficients. By Lemma 12, these equations are solvable for any polynomials $\mathrm{Pol}_i(z)$. Thus, we have proved that, for an arbitrary positive integer α, the modified algorithm that we have presented here will produce a solution $\tilde{S}_{4^{\alpha}}(z)$ to (14.4) modulo $2^{4^{\alpha}}$ which is a polynomial in $\tilde{\Phi}_2(z)$ of degree at most $4^{\alpha+1}-1$ with coefficients that are Laurent polynomials in z. □

Again, we have implemented the algorithm described in the above proof. For $\alpha = 1$, that is, for the modulus 16, we obtain the following result.

Theorem 37. *Let $\Phi_2(z) = \sum_{n\ge 0} z^{4^n/3}$, as before. Then, for the generating function $S_{\mathfrak{H}(5)}(z) = \sum_{n=0}^{\infty} s_{n+1}(\mathfrak{H}(5)) z^n$ for the subgroup numbers of $\mathfrak{H}(5)$, we have*

$$\begin{aligned} S_{\mathfrak{H}(5)}(z) &= 8z^{12} + 4z^9 + 8z^7 + 8z^5 + 2z^4 + 8z^2 + 4z + 14 + \frac{7}{z^3} \\ &\quad + \left(8z^{20/3} + 8z^{5/3} + \frac{8}{z^{1/3}} + \frac{8}{z^{4/3}} + \frac{12}{z^{10/3}}\right) \Phi_2(z) \\ &\quad + \left(8z^{19/3} + 8z^{4/3} + \frac{12}{z^{2/3}} + \frac{8}{z^{5/3}} + \frac{10}{z^{11/3}}\right) \Phi_2^2(z) + \left(8z^6 + 8z + \frac{8}{z} + \frac{12}{z^4}\right) \Phi_2^3(z) \\ &\quad + \left(8z^{32/3} + 8z^{20/3} + 8z^{11/3} + 8z^{8/3} + 8z^{5/3} + \frac{6}{z^{4/3}} + \frac{8}{z^{7/3}} + \frac{12}{z^{10/3}} + \frac{7}{z^{13/3}}\right) \Phi_2^4(z) \end{aligned}$$

$$\left(+\frac{8}{z^{2/3}}+\frac{8}{z^{5/3}}+\frac{8}{z^{8/3}}+\frac{4}{z^{11/3}}\right)\Phi_2^5(z)+\left(8z^6+8z+\frac{8}{z}+\frac{12}{z^2}+\frac{4}{z^4}\right)\Phi_2^6(z)$$
$$+\left(\frac{8}{z^{4/3}}+\frac{8}{z^{7/3}}+\frac{12}{z^{13/3}}\right)\Phi_2^7(z)$$
$$+\big(8z^{22/3}+8z^{19/3}+8z^{16/3}+8z^{10/3}+12z^{7/3}+8z^{4/3}$$
$$+\frac{4}{z^{2/3}}+\frac{8}{z^{5/3}}+\frac{5}{z^{8/3}}+\frac{2}{z^{11/3}}\Big)\Phi_2^8(z)$$
$$+\left(8z^6+8z+\frac{8}{z}+\frac{4}{z^4}+\frac{8}{z^2}\right)\Phi_2^9(z)+\left(\frac{12}{z^{4/3}}+\frac{2}{z^{13/3}}\right)\Phi_2^{10}(z)+\frac{8}{z^{8/3}}\Phi_2^{11}(z)$$
$$+\left(8z^6+8z^4+8z+8+\frac{8}{z}+\frac{12}{z^2}+\frac{12}{z^3}+\frac{12}{z^4}\right)\Phi_2^{12}(z)$$
$$+\left(\frac{8}{z^{4/3}}+\frac{8}{z^{7/3}}+\frac{12}{z^{13/3}}\right)\Phi_2^{13}(z)+\left(\frac{4}{z^{8/3}}+\frac{8}{z^{11/3}}\right)\Phi_2^{14}(z)\quad\text{modulo 16.}\quad(14.11)$$

We conjecture that Theorems 21 and 36 extend to any Hecke group $\mathfrak{H}(q)$, where q is a Fermat prime (note that $PSL_2(\mathbb{Z})\cong C_2*C_3=\mathfrak{H}(3)$).

Conjecture 38. *For a positive integer h, let $\Phi_h(z)=\sum_{n\geq 0}z^{2^{nh}/(2^h-1)}$. Let α be a further positive integer, and let $q=2^{2^f}+1$ be a Fermat prime. Then the generating function $S_{\mathfrak{H}(q)}(z)$ (see the first paragraph of Section 9 for the definition), reduced modulo $2^{2^{\alpha 2^f}}$, can be expressed as a polynomial in $\Phi_{2^f}(z)$ of degree at most $2^{(\alpha+1)2^f}-1$ with coefficients that are Laurent polynomials in $z^{1/(q-2)}$ over the integers.*

Note that Theorems 21 and 36 are the special cases corresponding to $f=0$ and $f=1$, respectively. In particular, we conjecture that the obvious extension of the algorithm described in the proofs of the two theorems would be successful modulo any 2-power. In more detail, given a Fermat prime q, the first step consists in deriving a recurrence relation for the Hadamard product of the sequences $\big(h_{C_2}(n)\big)_{n\geq 0}$ and $\big(h_{C_q}(n)/n!\big)_{n\geq 0}$. By the procedure explained in the paragraph containing (11.2) (where we now use (11.1) with $\Gamma=\mathfrak{H}(q)$), this leads to a Riccati-type differential equation for the generating function $\sum_{n\geq 0}s_{n+1}(\mathfrak{H}(q))\,z^n$ for the subgroup numbers of $\mathfrak{H}(q)$. The open questions are whether it will be possible to complete the base step, and whether it will always be possible to carry out the subsequent iterative steps in (the variation of) our method or, if necessary, its enhancement outlined in Appendix D. Given the description of the parity pattern of the subgroup numbers proved in [27, Theorem B], it is highly probable that the first question has a positive answer. What the answer to the second question is, remains entirely open. (The reader should recall that, in Section 12, we met a case where our method worked initially, but then stopped to work for modulus 16).

A Expansions of powers of the 2-power series $\Phi(z)$

Recall the notation

$$H_{a_1,a_2,\ldots,a_r}(z) = \sum_{n_1>n_2>\cdots>n_r\geq 0} z^{a_1 2^{n_1}+a_2 2^{n_2}+\cdots+a_r 2^{n_r}}$$

from Section 3. In this appendix we list the expansions of $\Phi^K(z)$ for $K = 5, 6, 7, 8$ in terms of the series $H_{a_1,a_2,\ldots,a_r}(z)$ where all a_i's are odd, obtained by using the algorithm described in Section 3 (see (3.1) and the proof of Lemma 9). Namely, we have

$$\begin{aligned}\Phi^5(z) = {} & 16H_5(z) - 40H_{3,1,1}(z) - 40H_{1,3,1}(z) - 40H_{1,1,3}(z) + 120H_{1,1,1,1,1}(z)\\ & - 80H_{3,1}(z) - 80H_{1,3}(z) + 240H_{1,1,1,1}(z) + (20z-90)H_3(z)\\ & - (60z-270)H_{1,1,1}(z) - (120z-190)H_{1,1}(z)\\ & + (25z^2-125z+75)H_1(z) + 50z^2 - 75z,\end{aligned}$$

$$\begin{aligned}\Phi^6(z) = {} & 96H_{5,1}(z) + 96H_{1,5}(z) + 80H_{3,3}(z) - 240H_{3,1,1,1}(z) - 240H_{1,3,1,1}(z)\\ & - 240H_{1,1,3,1}(z) - 240H_{1,1,1,3}(z) + 720H_{1,1,1,1,1,1}(z) + 240H_5(z)\\ & - 600H_{3,1,1}(z) - 600H_{1,3,1}(z) - 600H_{1,1,3}(z) + 1800H_{1,1,1,1,1}(z)\\ & + (120z-840)H_{3,1}(z) + (120z-840)H_{1,3}(z) - (360z-2520)H_{1,1,1,1}(z)\\ & + (300z-764)H_3(z) - (900z-2340)H_{1,1,1}(z) + (150z^2-1200z+1470)H_{1,1}(z)\\ & + (375z^2-1020z+525)H_1(z) - 61z^3 + 495z^2 - 525z,\end{aligned}$$

$$\begin{aligned}\Phi^7(z) = {} & -272H_7(z) + 672H_{5,1,1}(z) + 672H_{1,5,1}(z) + 672H_{1,1,5}(z)\\ & + 560H_{3,3,1}(z) + 560H_{3,1,3}(z) + 560H_{1,3,3}(z) + 2016H_{5,1}(z) + 2016H_{1,5}(z) + 1680H_{3,3}(z)\\ & - 1680H_{3,1,1,1,1}(z) - 1680H_{1,3,1,1,1}(z) - 1680H_{1,1,3,1,1}(z) - 1680H_{1,1,1,3,1}(z) - 1680H_{1,1,1,1,3}(z)\\ & + 5040H_{1,1,1,1,1,1,1}(z) - 5040H_{3,1,1,1}(z) - 5040H_{1,3,1,1}(z) - 5040H_{1,1,3,1}(z) - 5040H_{1,1,1,3}(z)\\ & + 15120H_{1,1,1,1,1,1}(z) - (336z-3360)H_5(z) + (840z-8400)H_{3,1,1}(z) + (840z-8400)H_{1,3,1}(z)\\ & + (840z-8400)H_{1,1,3}(z) - (2520z-25200)H_{1,1,1,1,1}(z) + (2520z-9408)H_{3,1}(z)\\ & + (2520z-9408)H_{1,3}(z) - (7560z-28560)H_{1,1,1,1}(z) - (350z^2-4060z+7434)H_3(z)\\ & + (1050z^2-12180z+23310)H_{1,1,1}(z) + (3150z^2-13020z+13230)H_{1,1}(z)\\ & - (427z^3-5040z^2+9555z-4347)H_1(z) - 1281z^3 + 5208z^2 - 4347z,\end{aligned}$$

$$\begin{aligned}
\Phi^8(z) &= -2176H_{7,1}(z) - 2176H_{1,7}(z) - 1792H_{5,3}(z) - 1792H_{3,5}(z) \\
&+ 5376H_{5,1,1,1}(z) + 5376H_{1,5,1,1}(z) + 5376H_{1,1,5,1}(z) + 5376H_{1,1,1,5}(z) + 4480H_{3,3,1,1}(z) \\
&+ 4480H_{3,1,3,1}(z) + 4480H_{3,1,1,3}(z) + 4480H_{1,3,3,1}(z) + 4480H_{1,3,1,3}(z) + 4480H_{1,1,3,3}(z) \\
&- 13440H_{3,1,1,1,1,1}(z) - 13440H_{1,3,1,1,1,1}(z) - 13440H_{1,1,3,1,1,1}(z) - 13440H_{1,1,1,3,1,1}(z) \\
&- 13440H_{1,1,1,1,3,1}(z) - 13440H_{1,1,1,1,1,3}(z) + 40320H_{1,1,1,1,1,1,1,1}(z) - 7616H_7(z) \\
&+ 18816H_{5,1,1}(z) + 18816H_{1,5,1}(z) + 18816H_{1,1,5}(z) \\
&+ 15680H_{3,3,1}(z) + 15680H_{3,1,3}(z) + 15680H_{1,3,3}(z) - 47040H_{3,1,1,1,1}(z) \\
&- 47040H_{1,3,1,1,1}(z) - 47040H_{1,1,3,1,1}(z) - 47040H_{1,1,1,3,1}(z) - 47040H_{1,1,1,1,3}(z) \\
&+ 141120H_{1,1,1,1,1,1,1}(z) - (2688z - 36288)H_{5,1}(z) - (2688z - 36288)H_{1,5}(z) \\
&- (2240z - 30240)H_{3,3}(z) + (6720z - 90720)H_{3,1,1,1}(z) + (6720z - 90720)H_{1,3,1,1}(z) \\
&+ (6720z - 90720)H_{1,1,3,1}(z) + (6720z - 90720)H_{1,1,1,3}(z) - (20160z - 272160)H_{1,1,1,1,1,1}(z) \\
&- (9408z - 47264)H_5(z) + (23520z - 119504)H_{3,1,1}(z) + (23520z - 119504)H_{1,3,1}(z) \\
&+ (23520z - 119504)H_{1,1,3}(z) - (70560z - 361200)H_{1,1,1,1,1}(z) \\
&- (2800z^2 - 44240z + 115304)H_{3,1}(z) - (2800z^2 - 44240z + 115304)H_{1,3}(z) \\
&+ (8400z^2 - 132720z + 355320)H_{1,1,1,1}(z) - (9800z^2 - 55832z + 80892)H_3(z) \\
&+ (29400z^2 - 168840z + 260820)H_{1,1,1}(z) - (3416z^3 - 55020z^2 + 154980z - 135982)H_{1,1}(z) \\
&- (11956z^3 - 68474z^2 + 101206z - 41245)H_1(z) + 1385z^4 - 22358z^3 + 59961z^2 - 41245z.
\end{aligned}$$

B The coefficients in the differential equation (11.5)

Here we provide explicit expressions for the coefficients in the Riccati-type differential equation (11.5), when reduced modulo 16:

$$\begin{aligned}
p_0(z) &= 8z^{47} + 8z^{46} + 12z^{45} + 4z^{43} + 12z^{41} + 12z^{40} + 4z^{39} + 12z^{38} + 8z^{37} + 4z^{36} + 4z^{34} + 2z^{33} \\
&+ 11z^{31} + 6z^{30} + 14z^{29} + 14z^{28} + 13z^{27} + 6z^{26} + 9z^{25} + 11z^{24} + 4z^{23} + 7z^{22} + 9z^{21} + z^{20} \\
&+ 7z^{19} + 15z^{18} + 14z^{17} + 12z^{16} + 11z^{15} + z^{14} + 10z^{13} + 5z^{12} + 2z^{11} + 8z^{10} + 9z^9 + 15z^8 \\
&+ 5z^7 + 13z^6 + 4z^4 + 14z^3 + z^2 + 11z + 15, \\
p_1(z) &= 8z^{48} + 12z^{46} + 12z^{45} + 4z^{43} + 12z^{42} + 4z^{41} + 4z^{40} + 4z^{39} + 8z^{38} + 4z^{36} + 13z^{34} + 6z^{33} \\
&+ 10z^{31} + z^{30} + 4z^{29} + 11z^{28} + 8z^{27} + 13z^{25} + z^{24} + 8z^{23} + z^{22} + z^{21} + 4z^{20} + 14z^{19} \\
&+ 9z^{18} + 6z^{17} + 14z^{16} + 8z^{15} + 13z^{14} + 6z^{13} + 2z^{12} + 9z^{10} + 11z^9 + 6z^7 + 8z^6 + 6z^5 \\
&+ 5z^4 + 3z^2 + 4z + 1,
\end{aligned}$$

$$
\begin{aligned}
p_2(z) &= 12z^{51} + 2z^{49} + 12z^{48} + 4z^{47} + 4z^{46} + 12z^{44} + 10z^{43} + 2z^{42} + 4z^{41} + 8z^{40} + 14z^{39} \\
&\quad + 5z^{37} + 2z^{36} + 6z^{35} + 10z^{34} + 8z^{33} + 10z^{32} + 5z^{31} + 7z^{30} + 12z^{29} + 7z^{28} + 4z^{27} \\
&\quad + 12z^{26} + 9z^{25} + 12z^{24} + 2z^{23} + 14z^{22} + 10z^{21} + 12z^{20} + 10z^{19} + 3z^{18} + 6z^{16} + 9z^{15} \\
&\quad + 12z^{14} + 15z^{13} + 14z^{12} + 10z^{11} + 2z^{10} + 12z^9 + 14z^8 + 13z^7 + 7z^6 + 8z^5 + z^3 + 2z^2, \\
p_3(z) &= 6z^{52} + 8z^{50} + 12z^{48} + 8z^{47} + 14z^{46} + 4z^{45} + 8z^{44} + 6z^{43} + 8z^{42} + 4z^{41} + 5z^{40} + 6z^{39} \\
&\quad + 12z^{38} + 2z^{37} + 2z^{36} + 7z^{34} + 6z^{33} + 7z^{31} + 14z^{30} + 8z^{29} + 5z^{28} + 14z^{27} + 8z^{26} \\
&\quad + 14z^{25} + 14z^{24} + 2z^{22} + 8z^{21} + 12z^{20} + 14z^{19} + 6z^{18} + 12z^{17} + 9z^{16} + 4z^{15} + 2z^{13} \\
&\quad + 2z^{12} + 15z^{10} + 14z^9, \\
p_4(z) &= 4z^{53} + 15z^{51} + 4z^{47} + 2z^{46} + z^{45} + 9z^{44} + 15z^{42} + 4z^{41} + 10z^{40} + 4z^{39} + 6z^{38} + 4z^{37} \\
&\quad + 2z^{36} + 6z^{35} + 10z^{34} + 11z^{33} + 8z^{32} + 8z^{31} + 10z^{29} + 12z^{26} + 12z^{25} + 2z^{23} + 4z^{22}, \\
p_5(z) &= 13z^{54} + 15z^{48} + 6z^{47} + 12z^{46} + 3z^{45} + 10z^{44} + 4z^{43} + 12z^{42} + 10z^{41} + 2z^{39} + 2z^{38} \\
&\quad + 15z^{36} + 14z^{35}, \\
p_6(z) &= 12z^{51} + 2z^{49} + 12z^{48} + 4z^{47} + 4z^{46} + 12z^{44} + 10z^{43} + 2z^{42} + 4z^{41} + 8z^{40} + 14z^{39} \\
&\quad + 5z^{37} + 2z^{36} + 6z^{35} + 10z^{34} + 8z^{33} + 10z^{32} + 5z^{31} + 7z^{30} + 12z^{29} + 7z^{28} + 4z^{27} \\
&\quad + 12z^{26} + 9z^{25} + 12z^{24} + 2z^{23} + 14z^{22} + 10z^{21} + 12z^{20} + 10z^{19} + 3z^{18} + 6z^{16} \\
&\quad + 9z^{15} + 12z^{14} + 15z^{13} + 14z^{12} + 10z^{11} + 2z^{10} + 12z^9 + 14z^8 + 13z^7 \\
&\quad + 7z^6 + 8z^5 + z^3 + 2z^2, \\
p_7(z) &= 12z^{53} + 13z^{51} + 12z^{47} + 6z^{46} + 3z^{45} + 11z^{44} + 13z^{42} + 12z^{41} + 14z^{40} + 12z^{39} + 2z^{38} \\
&\quad + 12z^{37} + 6z^{36} + 2z^{35} + 14z^{34} + z^{33} + 8z^{32} + 8z^{31} + 14z^{29} + 4z^{26} + 4z^{25} + 6z^{23} + 12z^{22}, \\
p_8(z) &= 2z^{52} + 8z^{50} + 4z^{48} + 8z^{47} + 10z^{46} + 12z^{45} + 8z^{44} + 2z^{43} + 8z^{42} + 12z^{41} + 15z^{40} + 2z^{39} \\
&\quad + 4z^{38} + 6z^{37} + 6z^{36} + 5z^{34} + 2z^{33} + 5z^{31} + 10z^{30} + 8z^{29} + 15z^{28} + 10z^{27} + 8z^{26} \\
&\quad + 10z^{25} + 10z^{24} + 6z^{22} + 8z^{21} + 4z^{20} + 10z^{19} + 2z^{18} + 4z^{17} + 11z^{16} + 12z^{15} \\
&\quad + 6z^{13} + 6z^{12} + 13z^{10} + 10z^9, \\
p_9(z) &= 8z^{53} + 10z^{51} + 8z^{47} + 12z^{46} + 6z^{45} + 6z^{44} + 10z^{42} + 8z^{41} + 12z^{40} + 8z^{39} + 4z^{38} + 8z^{37} \\
&\quad + 12z^{36} + 4z^{35} + 12z^{34} + 2z^{33} + 12z^{29} + 8z^{26} + 8z^{25} + 12z^{23} + 8z^{22}, \\
p_{10}(z) &= 2z^{54} + 6z^{48} + 12z^{47} + 8z^{46} + 14z^{45} + 4z^{44} + 8z^{43} + 8z^{42} + 4z^{41} + 4z^{39} + 4z^{38} \\
&\quad + 6z^{36} + 12z^{35}, \\
p_{11}(z) &= 3z^{54} + z^{48} + 10z^{47} + 4z^{46} + 13z^{45} + 6z^{44} + 12z^{43} + 4z^{42} + 6z^{41} + 14z^{39} \\
&\quad + 14z^{38} + z^{36} + 2z^{35}, \\
p_{12}(z) &= 6z^{52} + 8z^{50} + 12z^{48} + 8z^{47} + 14z^{46} + 4z^{45} + 8z^{44} + 6z^{43} + 8z^{42} + 4z^{41} + 5z^{40} + 6z^{39} + 12z^{38} \\
&\quad + 2z^{37} + 2z^{36} + 7z^{34} + 6z^{33} + 7z^{31} + 14z^{30} + 8z^{29} + 5z^{28} + 14z^{27} + 8z^{26} + 14z^{25} + 14z^{24} \\
&\quad + 2z^{22} + 8z^{21} + 12z^{20} + 14z^{19} + 6z^{18} + 12z^{17} + 9z^{16} + 4z^{15} + 2z^{13} + 2z^{12} + 15z^{10} + 14z^9, \\
p_{13}(z) &= 12z^{51} + 8z^{46} + 4z^{45} + 4z^{44} + 12z^{42} + 8z^{40} + 8z^{38} + 8z^{36} + 8z^{35} + 8z^{34} + 12z^{33} \\
&\quad + 8z^{29} + 8z^{23}, \\
p_{14}(z) &= 2z^{54} + 6z^{48} + 12z^{47} + 8z^{46} + 14z^{45} + 4z^{44} + 8z^{43} + 8z^{42} + 4z^{41} + 4z^{39} \\
&\quad + 4z^{38} + 6z^{36} + 12z^{35}, \\
p_{15}(z) &= 2z^{54} + 6z^{48} + 12z^{47} + 8z^{46} + 14z^{45} + 4z^{44} + 8z^{43} + 8z^{42} + 4z^{41} + 4z^{39} \\
&\quad + 4z^{38} + 6z^{36} + 12z^{35},
\end{aligned}
$$

$$
\begin{aligned}
p_{16}(z) &= 4z^{53} + 15z^{51} + 4z^{47} + 2z^{46} + z^{45} + 9z^{44} + 15z^{42} + 4z^{41} + 10z^{40} + 4z^{39} + 6z^{38} + 4z^{37} + 2z^{36} \\
&\quad + 6z^{35} + 10z^{34} + 11z^{33} + 8z^{32} + 8z^{31} + 10z^{29} + 12z^{26} + 12z^{25} + 2z^{23} + 4z^{22}, \\
p_{17}(z) &= z^{54} + 11z^{48} + 14z^{47} + 12z^{46} + 15z^{45} + 2z^{44} + 4z^{43} + 12z^{42} + 2z^{41} + 10z^{39} + 10z^{38} \\
&\quad + 11z^{36} + 6z^{35}, \\
p_{18}(z) &= 13z^{54} + 15z^{48} + 6z^{47} + 12z^{46} + 3z^{45} + 10z^{44} + 4z^{43} + 12z^{42} + 10z^{41} + 2z^{39} + 2z^{38} \\
&\quad + 15z^{36} + 14z^{35}.
\end{aligned}
$$

C The coefficients in the differential equation (12.3)

Here we provide explicit expressions for the coefficients in the Riccati-type differential equation (12.3), when reduced modulo 16:

$$
\begin{aligned}
q_0(z) &= 8z^{50} + 8z^{49} + 4z^{47} + 12z^{46} + 8z^{44} + 10z^{43} + 2z^{42} + 2z^{41} + 12z^{40} + 12z^{38} + 7z^{37} + 11z^{36} \\
&\quad + 10z^{35} + 11z^{34} + 13z^{33} + 13z^{32} + 14z^{31} + 15z^{30} + 10z^{29} + 14z^{28} + 8z^{27} + 10z^{26} + 6z^{25} \\
&\quad + z^{23} + 4z^{22} + 8z^{20} + 14z^{19} + 12z^{18} + 8z^{17} + 9z^{16} + 4z^{15} + 6z^{14} + 8z^{13} + z^{12} + 14z^{11} \\
&\quad + 9z^{10} + 2z^9 + 14z^8 + 10z^7 + 4z^6 + 11z^5 + 4z^4 + 4z^3 + z^2 + 8z + 15, \\
q_1(z) &= 8z^{51} + 8z^{50} + 8z^{49} + 12z^{48} + 4z^{47} + 12z^{46} + 4z^{45} + 14z^{43} + 10z^{42} + 5z^{40} + 4z^{39} + 4z^{38} \\
&\quad + 9z^{37} + 4z^{36} + 14z^{35} + 5z^{34} + 14z^{33} + 13z^{31} + 5z^{30} + 4z^{29} + 14z^{28} + 6z^{27} + 5z^{26} \\
&\quad + 10z^{25} + 12z^{23} + 9z^{22} + 12z^{21} + 13z^{20} + 6z^{19} + z^{18} + 7z^{17} + 15z^{15} + 11z^{14} + 7z^{13} \\
&\quad + 5z^{12} + z^{11} + 6z^{10} + 10z^9 + 2z^8 + 4z^7 + 8z^6 + 2z^5 + 11z^4 + 4z^3 + 8z^2 + 7z + 1, \\
q_2(z) &= 8z^{57} + 8z^{56} + 8z^{55} + 8z^{54} + 8z^{53} + 12z^{51} + 10z^{50} + 12z^{49} + 8z^{48} + 10z^{47} + 15z^{46} + 4z^{45} \\
&\quad + 10z^{43} + z^{42} + 11z^{41} + z^{40} + 2z^{39} + z^{38} + 3z^{37} + 6z^{36} + 7z^{35} + 8z^{34} + z^{33} + 6z^{31} + 9z^{29} \\
&\quad + 14z^{28} + 11z^{27} + 5z^{26} + 2z^{24} + 6z^{23} + 4z^{22} + 6z^{21} + 13z^{20} + z^{19} + 10z^{18} + z^{17} + 10z^{15} \\
&\quad + 12z^{14} + z^{13} + 9z^{12} + 9z^{11} + 7z^{10} + 4z^9 + 12z^8 + 3z^7 + 2z^6 + 9z^5 + 3z^4 + 9z^3, \\
q_3(z) &= 14z^{56} + 2z^{55} + 14z^{54} + 11z^{52} + 6z^{51} + 10z^{50} + 11z^{49} + 2z^{48} + 15z^{47} + 6z^{46} + 10z^{45} + 9z^{44} \\
&\quad + 4z^{43} + 5z^{42} + 11z^{41} + 5z^{40} + 10z^{39} + 4z^{38} + 12z^{37} + 2z^{36} + 5z^{35} + z^{34} + 6z^{33} + 5z^{32} \\
&\quad + 13z^{31} + 12z^{30} + 3z^{29} + 10z^{28} + 13z^{27} + 14z^{26} + 4z^{25} + 12z^{24} + 8z^{23} + 9z^{22} + 6z^{21} \\
&\quad + 14z^{20} + 7z^{19} + 5z^{18} + 4z^{17} + 4z^{16} + 8z^{14} + 15z^{13} + 13z^{11} + 9z^9 + 7z^8 + z^6 + 4z^5, \\
q_4(z) &= 8z^{66} + 15z^{58} + 14z^{57} + 12z^{56} + 9z^{54} + 7z^{53} + 9z^{52} + 10z^{51} + 12z^{50} + z^{49} + 10z^{48} + 14z^{46} \\
&\quad + 6z^{45} + 6z^{44} + 6z^{43} + 14z^{42} + 11z^{41} + 13z^{40} + 10z^{39} + z^{38} + 13z^{37} + 7z^{36} + 2z^{34} \\
&\quad + 12z^{33} + 4z^{32} + 13z^{31} + 13z^{30} + 4z^{29} + 11z^{28} + 7z^{27} + 8z^{26} + 2z^{25} + 6z^{24} + 13z^{23} \\
&\quad + 11z^{21} + 2z^{20} + 9z^{19} + 6z^{18} + 2z^{17} + 15z^{16} + 5z^{15} + 3z^{14} + 14z^{13} + 2z^{12} + 10z^{11} \\
&\quad + 9z^{10} + 6z^9 + 12z^8, \\
q_5(z) &= 5z^{59} + 13z^{58} + 12z^{56} + z^{55} + 8z^{54} + 5z^{53} + 12z^{52} + 15z^{51} + 8z^{50} + 14z^{49} + 2z^{48} + 4z^{47} \\
&\quad + 4z^{46} + 10z^{45} + 12z^{44} + 8z^{43} + 4z^{41} + 2z^{40} + 8z^{38} + 12z^{37} + 2z^{36} + 12z^{35} + 8z^{34}, \\
q_6(z) &= 12z^{49} + 4z^{48} + 12z^{46} + 12z^{45} + 12z^{44} + 4z^{43} + 12z^{42} + 12z^{41} + 12z^{39} + 4z^{38} + 4z^{37} \\
&\quad + 4z^{36} + 4z^{32} + 4z^{31} + 12z^{27} + 12z^{24} + 12z^{22} + 12z^{21} + 12z^{20} + 12z^{19} + 12z^{18} + 4z^{15} \\
&\quad + 4z^{13} + 12z^{12} + 12z^{11} + 12z^{10} + 4z^9 + 4z^8 + 4z^7 + 12z^6 + 4z^5, \\
q_7(z) &= 10z^{58} + 6z^{54} + 10z^{53} + 6z^{52} + 6z^{49} + 2z^{41} + 14z^{40} + 6z^{38} + 14z^{37} + 10z^{36} + 14z^{31} \\
&\quad + 14z^{30} + 2z^{28} + 10z^{27} + 14z^{23} + 2z^{21} + 6z^{19} + 10z^{16} + 14z^{15} + 2z^{14} + 6z^{10},
\end{aligned}
$$

$$
\begin{aligned}
q_8(z) &= 10z^{56} + 6z^{55} + 10z^{54} + 9z^{52} + 2z^{51} + 14z^{50} + 9z^{49} + 6z^{48} + 5z^{47} + 2z^{46} + 14z^{45} + 3z^{44} \\
&\quad + 12z^{43} + 7z^{42} + 9z^{41} + 7z^{40} + 14z^{39} + 12z^{38} + 4z^{37} + 6z^{36} + 7z^{35} + 11z^{34} + 2z^{33} \\
&\quad + 7z^{32} + 15z^{31} + 4z^{30} + z^{29} + 14z^{28} + 15z^{27} + 10z^{26} + 12z^{25} + 4z^{24} + 3z^{22} + 2z^{21} \\
&\quad + 10z^{20} + 13z^{19} + 7z^{18} + 12z^{17} + 12z^{16} + 5z^{13} + 15z^{11} + 3z^9 + 13z^8 + 11z^6 + 12z^5, \\
q_9(z) &= 7z^{59} + 15z^{58} + 11z^{55} + 7z^{53} + 5z^{51} + 10z^{49} + 6z^{48} + 14z^{45} + 6z^{40} + 6z^{36}, \\
q_{10}(z) &= z^{58} + 7z^{54} + 9z^{53} + 7z^{52} + 15z^{49} + 5z^{41} + 3z^{40} + 15z^{38} + 3z^{37} + 9z^{36} + 3z^{31} + 3z^{30} \\
&\quad + 5z^{28} + 9z^{27} + 3z^{23} + 5z^{21} + 7z^{19} + z^{16} + 11z^{15} + 13z^{14} + 7z^{10}, \\
q_{11}(z) &= 12z^{55} + 4z^{51} + 12z^{50} + 4z^{47} + 12z^{46} + 4z^{45} + 12z^{43} + 4z^{42} + 4z^{41} + 4z^{38} + 12z^{34} \\
&\quad + 4z^{33} + 4z^{32} + 12z^{29} + 4z^{26} + 12z^{25} + 12z^{22} + 12z^{16} + 12z^{15} + 4z^{14} + 12z^{13} \\
&\quad + 12z^9 + 4z^8 + 4z^6, \\
q_{12}(z) &= 15z^{58} + 14z^{57} + 12z^{56} + 9z^{54} + 7z^{53} + 9z^{52} + 10z^{51} + 12z^{50} + z^{49} + 10z^{48} + 14z^{46} + 6z^{45} \\
&\quad + 6z^{44} + 6z^{43} + 14z^{42} + 11z^{41} + 13z^{40} + 10z^{39} + z^{38} + 13z^{37} + 7z^{36} + 2z^{34} + 12z^{33} + 4z^{32} \\
&\quad + 13z^{31} + 13z^{30} + 4z^{29} + 11z^{28} + 7z^{27} + 2z^{25} + 6z^{24} + 13z^{23} + 11z^{21} + 2z^{20} + 9z^{19} + 6z^{18} \\
&\quad + 2z^{17} + 15z^{16} + 5z^{15} + 3z^{14} + 14z^{13} + 2z^{12} + 10z^{11} + 9z^{10} + 6z^9 + 12z^8, \\
q_{13}(z) &= 10z^{59} + 10z^{58} + 2z^{55} + 10z^{53} + 14z^{51} + 12z^{49} + 4z^{48} + 4z^{45} + 4z^{40} + 4z^{36}, \\
q_{14}(z) &= 8z^{57} + 8z^{56} + 8z^{55} + 12z^{53} + 8z^{51} + 8z^{50} + 8z^{49} + 8z^{48} + 10z^{47} + 14z^{46} + 10z^{45} + 8z^{44} \\
&\quad + 9z^{43} + 12z^{42} + 2z^{41} + 6z^{40} + 11z^{39} + 3z^{38} + 12z^{37} + 8z^{36} + 7z^{35} + 2z^{34} + z^{33} + z^{32} \\
&\quad + 7z^{31} + 12z^{30} + 12z^{29} + z^{28} + z^{26} + 15z^{25} + 9z^{24} + 14z^{23} + z^{22} + 3z^{21} + 3z^{20} + 4z^{19} \\
&\quad + 7z^{17} + 7z^{16} + 6z^{15} + 3z^{14} + z^{13} + 3z^{12} + 2z^{11} + 14z^9 + 2z^8 + 6z^7 + 2z^5 + 14z^4 \\
&\quad + 6z^3 + 14z^2, \\
q_{15}(z) &= 12z^{55} + 12z^{54} + 8z^{50} + 2z^{49} + 14z^{48} + 8z^{47} + 10z^{46} + 10z^{45} + 10z^{44} + 14z^{43} + 10z^{42} + 10z^{41} \\
&\quad + 2z^{39} + 14z^{38} + 6z^{37} + 14z^{36} + 12z^{34} + 14z^{32} + 14z^{31} + 4z^{30} + 8z^{28} + 10z^{27} + 12z^{25} \\
&\quad + 10z^{24} + 12z^{23} + 2z^{22} + 2z^{21} + 2z^{20} + 2z^{19} + 10z^{18} + 8z^{17} + 4z^{16} + 6z^{15} + 8z^{14} + 14z^{13} \\
&\quad + 2z^{12} + 2z^{11} + 2z^{10} + 6z^9 + 14z^8 + 14z^7 + 2z^6 + 14z^5 + 12z^4, \\
q_{16}(z) &= 4z^{65} + 10z^{57} + 6z^{56} + 9z^{55} + 8z^{53} + 6z^{52} + 11z^{51} + 13z^{50} + 2z^{49} + 12z^{48} + 3z^{47} + 13z^{46} \\
&\quad + 3z^{45} + 10z^{44} + 13z^{43} + 3z^{42} + 3z^{41} + 2z^{40} + 4z^{39} + 7z^{38} + 4z^{37} + 6z^{36} + 6z^{35} + 5z^{34} \\
&\quad + 15z^{33} + 3z^{32} + 10z^{31} + 14z^{30} + z^{29} + 2z^{28} + 14z^{27} + 11z^{26} + 9z^{25} + 2z^{24} + 9z^{22} + 8z^{21} \\
&\quad + 2z^{20} + 8z^{19} + 10z^{18} + 12z^{17} + 9z^{16} + 5z^{15} + 11z^{14} + 5z^{13} + 8z^{12} + 10z^{10} + z^9 + 7z^8 \\
&\quad + 6z^7 + 7z^6, \\
q_{17}(z) &= 8z^{58} + 12z^{55} + 8z^{54} + 8z^{53} + 8z^{52} + 4z^{51} + 12z^{50} + 8z^{49} + 8z^{48} + 4z^{47} + 12z^{45} + 8z^{43} \\
&\quad + 8z^{42} + 12z^{41} + 8z^{40} + 12z^{39} + 8z^{38} + 4z^{36} + 4z^{35} + 8z^{34} + 4z^{33} + 12z^{32} + 8z^{31} + 4z^{29} \\
&\quad + 8z^{28} + 8z^{26} + 8z^{22} + 12z^{21} + 8z^{18} + 12z^{17} + 8z^{16}, \\
q_{18}(z) &= 6z^{60} + 11z^{59} + 4z^{57} + 10z^{56} + 11z^{55} + 2z^{54} + 4z^{53}, \\
q_{19}(z) &= 4z^{56} + 12z^{55} + 4z^{54} + 2z^{52} + 4z^{51} + 12z^{50} + 2z^{49} + 12z^{48} + 10z^{47} + 4z^{46} + 12z^{45} + 6z^{44} \\
&\quad + 14z^{42} + 2z^{41} + 14z^{40} + 12z^{39} + 12z^{36} + 14z^{35} + 6z^{34} + 4z^{33} + 14z^{32} + 14z^{31} + 2z^{29} \\
&\quad + 12z^{28} + 14z^{27} + 4z^{26} + 6z^{22} + 4z^{21} + 4z^{20} + 10z^{19} + 14z^{18} + 10z^{13} + 14z^{11} + 6z^9 \\
&\quad + 10z^8 + 6z^6, \\
q_{20}(z) &= 12z^{65} + 14z^{57} + 2z^{56} + 3z^{55} + 2z^{52} + 9z^{51} + 15z^{50} + 6z^{49} + 4z^{48} + z^{47} + 15z^{46} + z^{45}
\end{aligned}
$$

$$+ 14z^{44} + 15z^{43} + z^{42} + z^{41} + 6z^{40} + 12z^{39} + 13z^{38} + 12z^{37} + 2z^{36} + 2z^{35} + 7z^{34} + 5z^{33}$$
$$+ z^{32} + 14z^{31} + 10z^{30} + 11z^{29} + 6z^{28} + 10z^{27} + 9z^{26} + 3z^{25} + 6z^{24} + 3z^{22} + 6z^{20}$$
$$+ 14z^{18} + 4z^{17} + 3z^{16} + 7z^{15} + 9z^{14} + 7z^{13} + 14z^{10} + 11z^{9} + 13z^{8} + 2z^{7} + 13z^{6},$$

$$q_{21}(z) = 2z^{60} + 9z^{59} + 14z^{56} + 9z^{55} + 6z^{54},$$

$$q_{22}(z) = 3z^{58} + 5z^{54} + 11z^{53} + 5z^{52} + 13z^{49} + 15z^{41} + 9z^{40} + 13z^{38} + 9z^{37} + 11z^{36} + 9z^{31}$$
$$+ 9z^{30} + 15z^{28} + 11z^{27} + 9z^{23} + 15z^{21} + 5z^{19} + 3z^{16} + z^{15} + 7z^{14} + 5z^{10},$$

$$q_{23}(z) = 14z^{58} + 12z^{57} + 2z^{54} + 14z^{53} + 2z^{52} + 4z^{51} + 2z^{49} + 4z^{48} + 12z^{46} + 12z^{45} + 12z^{44} + 12z^{43}$$
$$+ 12z^{42} + 6z^{41} + 10z^{40} + 4z^{39} + 2z^{38} + 10z^{37} + 14z^{36} + 4z^{34} + 10z^{31} + 10z^{30} + 6z^{28}$$
$$+ 14z^{27} + 4z^{25} + 12z^{24} + 10z^{23} + 6z^{21} + 4z^{20} + 2z^{19} + 12z^{18} + 4z^{17} + 14z^{16} + 10z^{15}$$
$$+ 6z^{14} + 12z^{13} + 4z^{12} + 4z^{11} + 2z^{10} + 12z^{9},$$

$$q_{24}(z) = 4z^{59} + 4z^{58} + 4z^{55} + 4z^{53} + 12z^{51},$$

$$q_{25}(z) = 12z^{55} + 4z^{51} + 12z^{50} + 4z^{47} + 12z^{45} + 12z^{41} + 12z^{39} + 4z^{36} + 4z^{35} + 4z^{33} + 12z^{32} + 4z^{29}$$
$$+ 12z^{21} + 12z^{17},$$

$$q_{26}(z) = 12z^{60} + 6z^{59} + 4z^{56} + 6z^{55} + 4z^{54},$$

$$q_{27}(z) = 8z^{57} + 8z^{56} + 8z^{55} + 8z^{54} + 8z^{53} + 4z^{51} + 14z^{50} + 4z^{49} + 8z^{48} + 14z^{47} + 5z^{46} + 12z^{45}$$
$$+ 14z^{43} + 11z^{42} + 9z^{41} + 11z^{40} + 6z^{39} + 11z^{38} + z^{37} + 2z^{36} + 13z^{35} + 8z^{34} + 11z^{33} + 2z^{31}$$
$$+ 3z^{29} + 10z^{28} + 9z^{27} + 7z^{26} + 6z^{24} + 2z^{23} + 12z^{22} + 2z^{21} + 15z^{20} + 11z^{19} + 14z^{18}$$
$$+ 11z^{17} + 14z^{15} + 4z^{14} + 11z^{13} + 3z^{12} + 3z^{11} + 13z^{10} + 12z^{9} + 4z^{8} + z^{7} + 6z^{6}$$
$$+ 3z^{5} + z^{4} + 3z^{3},$$

$$q_{28}(z) = 4z^{56} + 12z^{55} + 4z^{54} + 2z^{52} + 4z^{51} + 12z^{50} + 2z^{49} + 12z^{48} + 10z^{47} + 4z^{46} + 12z^{45} + 6z^{44}$$
$$+ 8z^{43} + 14z^{42} + 2z^{41} + 14z^{40} + 12z^{39} + 8z^{38} + 8z^{37} + 12z^{36} + 14z^{35} + 6z^{34} + 4z^{33}$$
$$+ 14z^{32} + 14z^{31} + 8z^{30} + 2z^{29} + 12z^{28} + 14z^{27} + 4z^{26} + 8z^{25} + 8z^{24} + 6z^{22} + 4z^{21}$$
$$+ 4z^{20} + 10z^{19} + 14z^{18} + 8z^{17} + 8z^{16} + 10z^{13} + 14z^{11} + 6z^{9} + 10z^{8} + 6z^{6} + 8z^{5},$$

$$q_{29}(z) = 8z^{66} + 15z^{58} + 14z^{57} + 12z^{56} + 9z^{54} + 7z^{53} + 9z^{52} + 10z^{51} + 12z^{50} + z^{49} + 10z^{48} + 14z^{46}$$
$$+ 6z^{45} + 6z^{44} + 6z^{43} + 14z^{42} + 11z^{41} + 13z^{40} + 10z^{39} + z^{38} + 13z^{37} + 7z^{36} + 2z^{34}$$
$$+ 12z^{33} + 4z^{32} + 13z^{31} + 13z^{30} + 4z^{29} + 11z^{28} + 7z^{27} + 8z^{26} + 2z^{25} + 6z^{24} + 13z^{23}$$
$$+ 11z^{21} + 2z^{20} + 9z^{19} + 6z^{18} + 2z^{17} + 15z^{16} + 5z^{15} + 3z^{14} + 14z^{13} + 2z^{12} + 10z^{11}$$
$$+ 9z^{10} + 6z^{9} + 12z^{8},$$

$$q_{30}(z) = 12z^{59} + 12z^{58} + 12z^{55} + 12z^{53} + 4z^{51} + 8z^{49} + 8z^{48} + 8z^{45} + 8z^{40} + 8z^{36},$$

$$q_{31}(z) = 4z^{55} + 12z^{51} + 4z^{50} + 12z^{47} + 4z^{46} + 12z^{45} + 4z^{43} + 12z^{42} + 12z^{41} + 12z^{38} + 4z^{34} + 12z^{33}$$
$$+ 12z^{32} + 4z^{29} + 12z^{26} + 4z^{25} + 4z^{22} + 4z^{16} + 4z^{15} + 12z^{14} + 4z^{13} + 4z^{9} + 12z^{8} + 12z^{6},$$

$$q_{32}(z) = 5z^{58} + 10z^{57} + 4z^{56} + 3z^{54} + 13z^{53} + 3z^{52} + 14z^{51} + 4z^{50} + 11z^{49} + 14z^{48} + 10z^{46} + 2z^{45}$$
$$+ 2z^{44} + 2z^{43} + 10z^{42} + 9z^{41} + 15z^{40} + 14z^{39} + 11z^{38} + 15z^{37} + 13z^{36} + 6z^{34} + 4z^{33}$$
$$+ 12z^{32} + 15z^{31} + 15z^{30} + 12z^{29} + 9z^{28} + 13z^{27} + 6z^{25} + 2z^{24} + 15z^{23} + 9z^{21} + 6z^{20} + 3z^{19}$$
$$+ 2z^{18} + 6z^{17} + 5z^{16} + 7z^{15} + z^{14} + 10z^{13} + 6z^{12} + 14z^{11} + 3z^{10} + 2z^{9} + 4z^{8},$$

$$q_{33}(z) = 12z^{59} + 12z^{58} + 12z^{55} + 12z^{53} + 4z^{51},$$

$$q_{34}(z) = 2z^{55} + 10z^{54} + 4z^{50} + 3z^{49} + 13z^{48} + 4z^{47} + 7z^{46} + 7z^{45} + 15z^{44} + 5z^{43} + 15z^{42} + 15z^{41}$$
$$+ 8z^{40} + 11z^{39} + 13z^{38} + z^{37} + 5z^{36} + 8z^{35} + 2z^{34} + 5z^{32} + 5z^{31} + 14z^{30} + 8z^{29} + 4z^{28}$$

$$
\begin{aligned}
&+ 15z^{27} + 10z^{25} + 15z^{24} + 10z^{23} + 11z^{22} + 11z^{21} + 11z^{20} + 3z^{19} + 15z^{18} + 4z^{17} + 14z^{16}\\
&+ z^{15} + 12z^{14} + 13z^{13} + 11z^{12} + 11z^{11} + 11z^{10} + z^9 + 5z^8 + 13z^7 + 11z^6 + 5z^5 + 2z^4,\\
q_{35}(z) = {}& 12z^{65} + 14z^{57} + 2z^{56} + 3z^{55} + 8z^{53} + 2z^{52} + 9z^{51} + 15z^{50} + 6z^{49} + 4z^{48} + z^{47} + 15z^{46}\\
&+ z^{45} + 14z^{44} + 15z^{43} + z^{42} + z^{41} + 6z^{40} + 12z^{39} + 13z^{38} + 12z^{37} + 2z^{36} + 2z^{35} + 7z^{34}\\
&+ 5z^{33} + z^{32} + 14z^{31} + 10z^{30} + 11z^{29} + 6z^{28} + 10z^{27} + 9z^{26} + 3z^{25} + 6z^{24} + 3z^{22} + 8z^{21}\\
&+ 6z^{20} + 8z^{19} + 14z^{18} + 4z^{17} + 3z^{16} + 7z^{15} + 9z^{14} + 7z^{13} + 8z^{12} + 14z^{10} + 11z^9 + 13z^8\\
&+ 2z^7 + 13z^6,\\
q_{36}(z) = {}& 8z^{67} + 12z^{58} + 14z^{55} + 4z^{54} + 4z^{53} + 4z^{52} + 2z^{51} + 6z^{50} + 12z^{49} + 12z^{48} + 10z^{47} + 6z^{45}\\
&+ 8z^{44} + 12z^{43} + 12z^{42} + 6z^{41} + 12z^{40} + 6z^{39} + 4z^{38} + 2z^{36} + 10z^{35} + 12z^{34} + 2z^{33}\\
&+ 6z^{32} + 12z^{31} + 10z^{29} + 12z^{28} + 12z^{26} + 8z^{25} + 12z^{22} + 14z^{21} + 8z^{19} + 4z^{18} + 14z^{17}\\
&+ 4z^{16} + 8z^{15},\\
q_{37}(z) = {}& 4z^{60} + 2z^{59} + 8z^{57} + 12z^{56} + 2z^{55} + 12z^{54} + 8z^{53},\\
q_{38}(z) = {}& 5z^{58} + 10z^{57} + 4z^{56} + 3z^{54} + 13z^{53} + 3z^{52} + 14z^{51} + 4z^{50} + 11z^{49} + 14z^{48} + 10z^{46} + 2z^{45}\\
&+ 2z^{44} + 2z^{43} + 10z^{42} + 9z^{41} + 15z^{40} + 14z^{39} + 11z^{38} + 15z^{37} + 13z^{36} + 6z^{34} + 4z^{33}\\
&+ 12z^{32} + 15z^{31} + 15z^{30} + 12z^{29} + 9z^{28} + 13z^{27} + 6z^{25} + 2z^{24} + 15z^{23} + 9z^{21} + 6z^{20}\\
&+ 3z^{19} + 2z^{18} + 6z^{17} + 5z^{16} + 7z^{15} + z^{14} + 10z^{13} + 6z^{12} + 14z^{11} + 3z^{10} + 2z^9 + 4z^8,\\
q_{39}(z) = {}& 4z^{58} + 10z^{55} + 12z^{54} + 12z^{53} + 12z^{52} + 6z^{51} + 2z^{50} + 4z^{49} + 4z^{48} + 14z^{47} + 2z^{45} + 4z^{43}\\
&+ 4z^{42} + 2z^{41} + 4z^{40} + 2z^{39} + 12z^{38} + 6z^{36} + 14z^{35} + 4z^{34} + 6z^{33} + 2z^{32} + 4z^{31} + 14z^{29}\\
&+ 4z^{28} + 4z^{26} + 4z^{22} + 10z^{21} + 12z^{18} + 10z^{17} + 12z^{16},\\
q_{40}(z) = {}& 12z^{59} + 12z^{58} + 12z^{55} + 12z^{53} + 4z^{51},\\
q_{41}(z) = {}& 4z^{60} + 2z^{59} + 12z^{56} + 2z^{55} + 12z^{54},\\
q_{42}(z) = {}& 2z^{56} + 14z^{55} + 2z^{54} + 5z^{52} + 10z^{51} + 6z^{50} + 5z^{49} + 14z^{48} + z^{47} + 10z^{46} + 6z^{45} + 7z^{44}\\
&+ 12z^{43} + 11z^{42} + 5z^{41} + 11z^{40} + 6z^{39} + 12z^{38} + 4z^{37} + 14z^{36} + 11z^{35} + 15z^{34} + 10z^{33}\\
&+ 11z^{32} + 3z^{31} + 4z^{30} + 13z^{29} + 6z^{28} + 3z^{27} + 2z^{26} + 12z^{25} + 4z^{24} + 8z^{23} + 7z^{22} + 10z^{21}\\
&+ 2z^{20} + 9z^{19} + 11z^{18} + 12z^{17} + 12z^{16} + 8z^{14} + z^{13} + 3z^{11} + 7z^9 + 9z^8 + 15z^6 + 12z^5,\\
q_{43}(z) = {}& 8z^{66} + 3z^{58} + 6z^{57} + 12z^{56} + 5z^{54} + 11z^{53} + 5z^{52} + 2z^{51} + 12z^{50} + 13z^{49} + 2z^{48} + 6z^{46}\\
&+ 14z^{45} + 14z^{44} + 14z^{43} + 6z^{42} + 15z^{41} + 9z^{40} + 2z^{39} + 13z^{38} + 9z^{37} + 11z^{36} + 10z^{34}\\
&+ 12z^{33} + 4z^{32} + 9z^{31} + 9z^{30} + 4z^{29} + 15z^{28} + 11z^{27} + 8z^{26} + 10z^{25} + 14z^{24} + 9z^{23}\\
&+ 15z^{21} + 10z^{20} + 5z^{19} + 14z^{18} + 10z^{17} + 3z^{16} + z^{15} + 7z^{14} + 6z^{13} + 10z^{12} + 2z^{11}\\
&+ 5z^{10} + 14z^9 + 12z^8,\\
q_{44}(z) = {}& 2z^{59} + 2z^{58} + 8z^{56} + 10z^{55} + 2z^{53} + 8z^{52} + 6z^{51} + 12z^{49} + 4z^{48} + 8z^{47} + 8z^{46} + 4z^{45}\\
&+ 8z^{44} + 8z^{41} + 4z^{40} + 8z^{37} + 4z^{36} + 8z^{35},\\
q_{45}(z) = {}& 8z^{21},\\
q_{46}(z) = {}& 6z^{59} + 6z^{58} + 14z^{55} + 6z^{53} + 2z^{51} + 4z^{49} + 12z^{48} + 12z^{45} + 12z^{40} + 12z^{36},\\
q_{47}(z) = {}& 4z^{65} + 2z^{57} + 14z^{56} + 13z^{55} + 8z^{53} + 14z^{52} + 7z^{51} + z^{50} + 10z^{49} + 12z^{48} + 15z^{47} + z^{46}\\
&+ 15z^{45} + 2z^{44} + z^{43} + 15z^{42} + 15z^{41} + 10z^{40} + 4z^{39} + 3z^{38} + 4z^{37} + 14z^{36} + 14z^{35} + 9z^{34}\\
&+ 11z^{33} + 15z^{32} + 2z^{31} + 6z^{30} + 5z^{29} + 10z^{28} + 6z^{27} + 7z^{26} + 13z^{25} + 10z^{24} + 13z^{22} + 8z^{21}\\
&+ 10z^{20} + 8z^{19} + 2z^{18} + 12z^{17} + 13z^{16} + 9z^{15} + 7z^{14} + 9z^{13} + 8z^{12} + 2z^{10} + 5z^9 + 3z^8
\end{aligned}
$$

$$+ 14z^7 + 3z^6,$$

$$q_{48}(z) = 8z^{58} + 4z^{55} + 8z^{54} + 8z^{53} + 8z^{52} + 12z^{51} + 4z^{50} + 8z^{49} + 8z^{48} + 12z^{47} + 4z^{45} + 8z^{43} + 8z^{42} + 4z^{41} + 8z^{40} + 4z^{39} + 8z^{38} + 12z^{36} + 12z^{35} + 8z^{34} + 12z^{33} + 4z^{32} + 8z^{31} + 12z^{29} + 8z^{28} + 8z^{26} + 8z^{22} + 4z^{21} + 8z^{18} + 4z^{17} + 8z^{16},$$

$$q_{49}(z) = 4z^{60} + 10z^{59} + 8z^{57} + 12z^{56} + 10z^{55} + 12z^{54} + 8z^{53},$$

$$q_{50}(z) = 4z^{59} + 4z^{58} + 4z^{55} + 4z^{53} + 12z^{51},$$

$$q_{51}(z) = 12z^{60} + 14z^{59} + 4z^{56} + 14z^{55} + 4z^{54},$$

$$q_{52}(z) = 8z^{66} + 7z^{58} + 14z^{57} + 12z^{56} + z^{54} + 15z^{53} + z^{52} + 10z^{51} + 12z^{50} + 9z^{49} + 10z^{48} + 14z^{46} + 6z^{45} + 6z^{44} + 6z^{43} + 14z^{42} + 3z^{41} + 5z^{40} + 10z^{39} + 9z^{38} + 5z^{37} + 15z^{36} + 2z^{34} + 12z^{33} + 4z^{32} + 5z^{31} + 5z^{30} + 4z^{29} + 3z^{28} + 15z^{27} + 8z^{26} + 2z^{25} + 6z^{24} + 5z^{23} + 3z^{21} + 2z^{20} + z^{19} + 6z^{18} + 2z^{17} + 7z^{16} + 13z^{15} + 11z^{14} + 14z^{13} + 2z^{12} + 10z^{11} + z^{10} + 6z^9 + 12z^8,$$

$$q_{53}(z) = 4z^{59} + 4z^{58} + 4z^{55} + 4z^{53} + 12z^{51} + 8z^{49} + 8z^{48} + 8z^{45} + 8z^{40} + 8z^{36},$$

$$q_{54}(z) = 4z^{67} + 14z^{58} + 8z^{57} + 15z^{55} + 10z^{54} + 10z^{53} + 2z^{52} + z^{51} + 11z^{50} + 14z^{49} + 6z^{48} + 5z^{47} + 8z^{46} + 3z^{45} + 12z^{44} + 6z^{43} + 6z^{42} + 3z^{41} + 6z^{40} + 3z^{39} + 2z^{38} + 9z^{36} + 5z^{35} + 6z^{34} + 9z^{33} + 3z^{32} + 6z^{31} + 8z^{30} + 13z^{29} + 6z^{28} + 6z^{26} + 4z^{25} + 8z^{24} + 14z^{22} + 15z^{21} + 4z^{19} + 2z^{18} + 15z^{17} + 10z^{16} + 4z^{15},$$

$$q_{55}(z) = 6z^{60} + 3z^{59} + 4z^{57} + 10z^{56} + 3z^{55} + 2z^{54} + 4z^{53},$$

$$q_{56}(z) = 5z^{59} + 13z^{58} + 12z^{56} + z^{55} + 8z^{54} + 5z^{53} + 12z^{52} + 15z^{51} + 8z^{50} + 14z^{49} + 2z^{48} + 4z^{47} + 4z^{46} + 10z^{45} + 12z^{44} + 8z^{43} + 4z^{41} + 2z^{40} + 8z^{38} + 12z^{37} + 2z^{36} + 12z^{35} + 8z^{34},$$

$$q_{57}(z) = 14z^{60} + 15z^{59} + 4z^{57} + 2z^{56} + 15z^{55} + 10z^{54} + 4z^{53},$$

$$q_{58}(z) = 8z^{57} + 8z^{56} + 8z^{55} + 12z^{53} + 8z^{51} + 8z^{50} + 8z^{49} + 8z^{48} + 10z^{47} + 14z^{46} + 10z^{45} + 8z^{44} + 9z^{43} + 12z^{42} + 2z^{41} + 6z^{40} + 11z^{39} + 3z^{38} + 12z^{37} + 8z^{36} + 7z^{35} + 2z^{34} + z^{33} + z^{32} + 7z^{31} + 12z^{30} + 12z^{29} + z^{28} + z^{26} + 15z^{25} + 9z^{24} + 14z^{23} + z^{22} + 3z^{21} + 3z^{20} + 4z^{19} + 7z^{17} + 7z^{16} + 6z^{15} + 3z^{14} + z^{13} + 3z^{12} + 2z^{11} + 14z^9 + 2z^8 + 6z^7 + 2z^5 + 14z^4 + 6z^3 + 14z^2,$$

$$q_{59}(z) = 4z^{56} + 12z^{55} + 4z^{54} + 2z^{52} + 4z^{51} + 12z^{50} + 2z^{49} + 12z^{48} + 10z^{47} + 4z^{46} + 12z^{45} + 6z^{44} + 14z^{42} + 2z^{41} + 14z^{40} + 12z^{39} + 12z^{36} + 14z^{35} + 6z^{34} + 4z^{33} + 14z^{32} + 14z^{31} + 2z^{29} + 12z^{28} + 14z^{27} + 4z^{26} + 6z^{22} + 4z^{21} + 4z^{20} + 10z^{19} + 14z^{18} + 10z^{13} + 14z^{11} + 6z^9 + 10z^8 + 6z^6,$$

$$q_{60}(z) = 12z^{65} + 14z^{57} + 2z^{56} + 3z^{55} + 2z^{52} + 9z^{51} + 15z^{50} + 6z^{49} + 4z^{48} + z^{47} + 15z^{46} + z^{45} + 14z^{44} + 15z^{43} + z^{42} + z^{41} + 6z^{40} + 12z^{39} + 13z^{38} + 12z^{37} + 2z^{36} + 2z^{35} + 7z^{34} + 5z^{33} + z^{32} + 14z^{31} + 10z^{30} + 11z^{29} + 6z^{28} + 10z^{27} + 9z^{26} + 3z^{25} + 6z^{24} + 3z^{22} + 6z^{20} + 14z^{18} + 4z^{17} + 3z^{16} + 7z^{15} + 9z^{14} + 7z^{13} + 14z^{10} + 11z^9 + 13z^8 + 2z^7 + 13z^6,$$

$$q_{61}(z) = 2z^{60} + 9z^{59} + 14z^{56} + 9z^{55} + 6z^{54},$$

$$q_{62}(z) = 3z^{58} + 5z^{54} + 11z^{53} + 5z^{52} + 13z^{49} + 15z^{41} + 9z^{40} + 13z^{38} + 9z^{37} + 11z^{36} + 9z^{31} + 9z^{30} + 15z^{28} + 11z^{27} + 9z^{23} + 15z^{21} + 5z^{19} + 3z^{16} + z^{15} + 7z^{14} + 5z^{10},$$

$$q_{63}(z) = 6z^{55} + 14z^{54} + 12z^{50} + 9z^{49} + 7z^{48} + 12z^{47} + 5z^{46} + 5z^{45} + 13z^{44} + 15z^{43} + 13z^{42} + 13z^{41} + 8z^{40} + z^{39} + 7z^{38} + 3z^{37} + 15z^{36} + 8z^{35} + 6z^{34} + 15z^{32} + 15z^{31} + 10z^{30}$$

$$+ 8z^{29} + 12z^{28} + 13z^{27} + 14z^{25} + 13z^{24} + 14z^{23} + z^{22} + z^{21} + z^{20} + 9z^{19} + 13z^{18}$$
$$+ 12z^{17} + 10z^{16} + 3z^{15} + 4z^{14} + 7z^{13} + z^{12} + z^{11} + z^{10} + 3z^9 + 15z^8 + 7z^7 + z^6$$
$$+ 15z^5 + 6z^4,$$

$$q_{64}(z) = 15z^{58} + 14z^{57} + 12z^{56} + 9z^{54} + 7z^{53} + 9z^{52} + 10z^{51} + 12z^{50} + z^{49} + 10z^{48} + 14z^{46} + 6z^{45}$$
$$+ 6z^{44} + 6z^{43} + 14z^{42} + 11z^{41} + 13z^{40} + 10z^{39} + z^{38} + 13z^{37} + 7z^{36} + 2z^{34} + 12z^{33} + 4z^{32}$$
$$+ 13z^{31} + 13z^{30} + 4z^{29} + 11z^{28} + 7z^{27} + 2z^{25} + 6z^{24} + 13z^{23} + 11z^{21} + 2z^{20} + 9z^{19} + 6z^{18}$$
$$+ 2z^{17} + 15z^{16} + 5z^{15} + 3z^{14} + 14z^{13} + 2z^{12} + 10z^{11} + 9z^{10} + 6z^9 + 12z^8,$$

$$q_{65}(z) = 12z^{58} + 14z^{55} + 4z^{54} + 4z^{53} + 4z^{52} + 2z^{51} + 6z^{50} + 12z^{49} + 12z^{48} + 10z^{47} + 6z^{45} + 12z^{43}$$
$$+ 12z^{42} + 6z^{41} + 12z^{40} + 6z^{39} + 4z^{38} + 2z^{36} + 10z^{35} + 12z^{34} + 2z^{33} + 6z^{32} + 12z^{31} + 10z^{29}$$
$$+ 12z^{28} + 12z^{26} + 12z^{22} + 14z^{21} + 4z^{18} + 14z^{17} + 4z^{16},$$

$$q_{66}(z) = 12z^{65} + 14z^{57} + 2z^{56} + 3z^{55} + 8z^{53} + 2z^{52} + 9z^{51} + 15z^{50} + 6z^{49} + 4z^{48} + z^{47} + 15z^{46} + z^{45}$$
$$+ 14z^{44} + 15z^{43} + z^{42} + z^{41} + 6z^{40} + 12z^{39} + 13z^{38} + 12z^{37} + 2z^{36} + 2z^{35} + 7z^{34} + 5z^{33}$$
$$+ z^{32} + 14z^{31} + 10z^{30} + 11z^{29} + 6z^{28} + 10z^{27} + 9z^{26} + 3z^{25} + 6z^{24} + 3z^{22} + 8z^{21} + 6z^{20}$$
$$+ 8z^{19} + 14z^{18} + 4z^{17} + 3z^{16} + 7z^{15} + 9z^{14} + 7z^{13} + 8z^{12} + 14z^{10} + 11z^9 + 13z^8$$
$$+ 2z^7 + 13z^6,$$

$$q_{67}(z) = 12z^{59} + 12z^{58} + 12z^{55} + 12z^{53} + 4z^{51},$$

$$q_{68}(z) = 4z^{60} + 2z^{59} + 12z^{56} + 2z^{55} + 12z^{54},$$

$$q_{69}(z) = 4z^{67} + 14z^{58} + 8z^{57} + 7z^{55} + 10z^{54} + 10z^{53} + 2z^{52} + 9z^{51} + 3z^{50} + 14z^{49} + 6z^{48} + 13z^{47}$$
$$+ 8z^{46} + 11z^{45} + 12z^{44} + 6z^{43} + 6z^{42} + 11z^{41} + 6z^{40} + 11z^{39} + 2z^{38} + z^{36} + 13z^{35} + 6z^{34}$$
$$+ z^{33} + 11z^{32} + 6z^{31} + 8z^{30} + 5z^{29} + 6z^{28} + 6z^{26} + 4z^{25} + 8z^{24} + 14z^{22} + 7z^{21} + 4z^{19}$$
$$+ 2z^{18} + 7z^{17} + 10z^{16} + 4z^{15},$$

$$q_{70}(z) = 14z^{60} + 15z^{59} + 4z^{57} + 2z^{56} + 15z^{55} + 10z^{54} + 4z^{53},$$

$$q_{71}(z) = 4z^{51} + 14z^{50} + 4z^{49} + 14z^{47} + 5z^{46} + 12z^{45} + 14z^{43} + 11z^{42} + 9z^{41} + 11z^{40} + 6z^{39} + 11z^{38}$$
$$+ z^{37} + 2z^{36} + 13z^{35} + 11z^{33} + 2z^{31} + 3z^{29} + 10z^{28} + 9z^{27} + 7z^{26} + 6z^{24} + 2z^{23} + 12z^{22}$$
$$+ 2z^{21} + 15z^{20} + 11z^{19} + 14z^{18} + 11z^{17} + 14z^{15} + 4z^{14} + 11z^{13} + 3z^{12} + 3z^{11} + 13z^{10}$$
$$+ 12z^9 + 4z^8 + z^7 + 6z^6 + 3z^5 + z^4 + 3z^3,$$

$$q_{72}(z) = 5z^{58} + 10z^{57} + 4z^{56} + 3z^{54} + 13z^{53} + 3z^{52} + 14z^{51} + 11z^{49} + 14z^{48} + 10z^{46} + 2z^{45} + 2z^{44}$$
$$+ 2z^{43} + 10z^{42} + 9z^{41} + 15z^{40} + 14z^{39} + 11z^{38} + 15z^{37} + 13z^{36} + 6z^{34} + 15z^{31} + 15z^{30}$$
$$+ 9z^{28} + 13z^{27} + 6z^{25} + 2z^{24} + 15z^{23} + 9z^{21} + 6z^{20} + 3z^{19} + 2z^{18} + 6z^{17} + 5z^{16} + 7z^{15}$$
$$+ z^{14} + 10z^{13} + 6z^{12} + 14z^{11} + 3z^{10} + 2z^9 + 4z^8,$$

$$q_{73}(z) = 2z^{55} + 6z^{51} + 10z^{50} + 6z^{47} + 10z^{46} + 6z^{45} + 10z^{43} + 6z^{42} + 6z^{41} + 14z^{38} + 10z^{34} + 14z^{33}$$
$$+ 6z^{32} + 2z^{29} + 6z^{26} + 2z^{25} + 2z^{22} + 2z^{16} + 10z^{15} + 6z^{14} + 10z^{13} + 2z^9 + 14z^8 + 14z^6,$$

$$q_{74}(z) = 2z^{55} + 10z^{54} + 4z^{50} + 3z^{49} + 13z^{48} + 4z^{47} + 7z^{46} + 7z^{45} + 15z^{44} + 5z^{43} + 15z^{42} + 15z^{41}$$
$$+ 11z^{39} + 13z^{38} + z^{37} + 5z^{36} + 2z^{34} + 5z^{32} + 5z^{31} + 14z^{30} + 4z^{28} + 15z^{27} + 10z^{25}$$
$$+ 15z^{24} + 10z^{23} + 11z^{22} + 11z^{21} + 11z^{20} + 3z^{19} + 15z^{18} + 4z^{17} + 14z^{16} + z^{15} + 12z^{14}$$
$$+ 13z^{13} + 11z^{12} + 11z^{11} + 11z^{10} + z^9 + 5z^8 + 13z^7 + 11z^6 + 5z^5 + 2z^4,$$

$$q_{75}(z) = 10z^{58} + 13z^{55} + 14z^{54} + 14z^{53} + 6z^{52} + 3z^{51} + z^{50} + 10z^{49} + 2z^{48} + 15z^{47} + 9z^{45} + 2z^{43}$$
$$+ 2z^{42} + 9z^{41} + 2z^{40} + 9z^{39} + 6z^{38} + 11z^{36} + 15z^{35} + 2z^{34} + 11z^{33} + 9z^{32} + 2z^{31} + 7z^{29}$$

$$+ 2z^{28} + 2z^{26} + 10z^{22} + 13z^{21} + 6z^{18} + 13z^{17} + 14z^{16},$$

$$q_{76}(z) = 5z^{52} + 5z^{49} + z^{47} + 7z^{44} + 11z^{42} + 5z^{41} + 11z^{40} + 11z^{35} + 15z^{34} + 11z^{32} + 3z^{31} + 13z^{29}$$
$$+ 3z^{27} + 7z^{22} + 9z^{19} + 11z^{18} + z^{13} + 3z^{11} + 7z^{9} + 9z^{8} + 15z^{6},$$

$$q_{77}(z) = 13z^{55} + 7z^{51} + z^{50} + 15z^{47} + z^{46} + 15z^{45} + z^{43} + 15z^{42} + 15z^{41} + 3z^{38} + 9z^{34} + 11z^{33}$$
$$+ 15z^{32} + 5z^{29} + 7z^{26} + 13z^{25} + 13z^{22} + 13z^{16} + 9z^{15} + 7z^{14} + 9z^{13} + 5z^{9} + 3z^{8} + 3z^{6}.$$

D The method "reloaded"

As the reader will recall from Section 4 (cf. Remark 11), our method described there is based on the "hope" that, if a polynomial in $\Phi(z)$ is zero modulo a 2-power 2^β (as a formal Laurent series), then already all coefficients of powers of $\Phi(z)$ in this polynomial vanish modulo 2^β. (This is manifest in each comparison of coefficients of powers of $\Phi(z)$ in Section 4.) In general, however, this implication does not hold (see Lemma 39 below for the case of modulus $2^4 = 16$). It may consequently happen that the method from Section 4 fails to find a solution modulo 2^β to a given differential equation in the form of a polynomial in $\Phi(z)$ with coefficients that are Laurent polynomials in z over the integers, while such a solution may in fact exist. As it turns out, this situation occurs when treating the subgroup numbers of $SL_2(\mathbb{Z})$ and of $\Gamma_3(3)$ modulo 16, see the paragraph above Theorem 28 and Remark 32. (In the former case, there is indeed a solution, while in the latter there is not.)

Our aim here is to explain how the method from Section 4 can be enhanced so that one can *decide* whether or not such a solution modulo a given 2-power 2^β exists; and, if it exists, how to find it. In principle, it should be possible to describe such an improved method for an arbitrary 2-power 2^β. Since, in the present paper, we need it only for the modulus 16, and since we are not able to rigorously establish the validity of the enhancement we have in mind in general (it would depend on Conjecture 4, which at present we are not able to prove), we content ourselves with describing the enhanced method for the modulus 16. From this description, the reader should have no difficulty to "extrapolate" to arbitrary 2-powers, assuming the truth of Conjecture 4.

We begin by characterising when a polynomial in $\Phi(z)$ with coefficients that are Laurent polynomials in z over the integers vanishes modulo 16 as a Laurent series in z.

Lemma 39. *As before, let $\Phi(z) = \sum_{n\geq 0} z^{2^n}$. Furthermore, let $P(z, \Phi(z))$ be a polynomial in $\Phi(z)$ with coefficients that are Laurent polynomials in z over the integers. Then, as a Laurent series in z,*

$$P(z, \Phi(z)) = 0 \quad \text{modulo } 16$$

if, and only if, the coefficients of powers of Φ in $P(z, \Phi(z))$ agree modulo 16 with the corresponding ones in

$$c_1(z)M_{16}(z, \Phi(z)) + 2\big(c_2(z)\Phi(z) + c_3(z)\big)M_8(z, \Phi(z)) + 8\big(c_4(z)\Phi(z) + c_5(z)\big)M_2(z, \Phi(z)). \quad \text{(D.1)}$$

Here, $M_2(z,t), M_8(z,t), M_{16}(z,t)$ are the minimal polynomials for the moduli $2, 8, 16$, respectively, given in Proposition 2, and $c_1(z), c_2(z), c_3(z), c_4(z), c_5(z)$ are suitable Laurent polynomials in z over the integers.

Proof. We assume that $P(z, \Phi(z)) = 0$ modulo 16.

Recall that, by definition, $M_{16}(z, \Phi(z))$ is a *monic* polynomial in $\Phi(z)$. We use this fact to perform division of $P(z, \Phi(z))$ by $M_{16}(z, \Phi(z))$ (as polynomials in $\Phi(z)$), thus obtaining

$$P(z, \Phi(z)) = c_1(z) M_{16}(z) + P_1(z, \Phi(z)), \tag{D.2}$$

where $P_1(z, \Phi(z))$ is a polynomial in $\Phi(z)$ of degree at most 5, with coefficients that are Laurent polynomials in z over the integers, say

$$P_1(z, \Phi(z)) = d_5(z)\Phi^5(z) + d_4(z)\Phi^4(z) + d_3(z)\Phi^3(z) + d_2(z)\Phi^2(z) + d_1(z)\Phi(z) + d_0(z). \tag{D.3}$$

As Laurent series in z, both $P(z, \Phi(z))$ and $M_{16}(z, \Phi(z))$ vanish modulo 16. Using this observation in (D.2), we see that $P_1(z, \Phi(z))$ vanishes modulo 16 as well. Now recall from (2.5) and the proof of Lemma 1 that

$$P_1(z, \Phi(z)) = d_5(z)\, 5!\, E_5(z) + Q_1(z)$$

(with a suitable series $Q_1(z)$), where $D(Q_1(z), 16; n)$ has strictly smaller asymptotic growth (in n) than $D(E_5(z), 16; n)$. Since, as we already observed, $P_1(z, \Phi(z))$ vanishes modulo 16, it follows that $5! d_5(z)$ must vanish modulo 16, that is, there exists a Laurent polynomial $c_2(z)$ over the integers such that $d_5(z) = 2c_2(z)$. We use this observation in (D.3) to see that

$$P(z, \Phi(z)) = c_1(z) M_{16}(z) + 2c_2(z)\Phi(z) M_8(z, \Phi(z)) + P_2(z, \Phi(z)), \tag{D.4}$$

where $P_2(z, \Phi(z))$ is a polynomial in $\Phi(z)$ of degree at most 4, with coefficients that are Laurent polynomials in z over the integers, say

$$P_2(z, \Phi(z)) = e_4(z)\Phi^4(z) + e_3(z)\Phi^3(z) + e_2(z)\Phi^2(z) + e_1(z)\Phi(z) + e_0(z).$$

Applying the same kind of argument again, we further deduce that

$$P(z, \Phi(z)) = c_1(z) M_{16}(z) + 2\big(c_2(z)\Phi(z) + c_3(z)\big) M_8(z, \Phi(z)) + P_3(z, \Phi(z)), \tag{D.5}$$

where $c_3(z)$ is a Laurent polynomial in z over the integers and $P_3(z, \Phi(z))$ is a polynomial in $\Phi(z)$ of degree at most 3, with coefficients that are Laurent polynomials in z over the integers, say

$$P_3(z, \Phi(z)) = f_3(z)\Phi^3(z) + f_2(z)\Phi^2(z) + f_1(z)\Phi(z) + f_0(z).$$

As Laurent series in z, all of $P(z, \Phi(z))$, $M_{16}(z, \Phi(z))$, and $2M_8(z, \Phi(z))$ vanish modulo 16. Using this observation in (D.5), we see that $P_3(z, \Phi(z))$ vanishes modulo 16 as well. Equation (2.5) and the proof of Lemma 1 give that

$$P_3(z, \Phi(z)) = d_3(z)\, 3!\, E_3(z) + Q_3(z)$$

(with a suitable series $Q_3(z)$), where $D(Q_3(z),16;n)$ has strictly smaller asymptotic growth (in n) than $D(E_3(z),16;n)$. Since, as we already observed, $P_3(z,\Phi(z))$ vanishes modulo 16, it follows that $3!d_3(z)$ must vanish modulo 16, that is, there exists a Laurent polynomial $c_4(z)$ over the integers such that $d_3(z) = 8c_4(z)$. By another application of the same kind of argument, this leads to

$$P(z,\Phi(z)) = c_1(z)M_{16}(z) + 2\big(c_2(z)\Phi(z) + c_3(z)\big)M_8(z,\Phi(z)) \\ + 8\big(c_4(z)\Phi(z) + c_5(z)\big)M_2(z,\Phi(z)) + P_4(z,\Phi(z)), \quad \text{(D.6)}$$

where $c_5(z)$ is a Laurent polynomial in z over the integers and $P_4(z,\Phi(z))$ is a polynomial in $\Phi(z)$ of degree at most 1, with coefficients that are Laurent polynomials in z over the integers, say

$$P_4(z,\Phi(z)) = g_1(z)\Phi(z) + g_0(z).$$

Since $P(z,\Phi(z))$, $M_{16}(z,\Phi(z))$, $2M_8(z,\Phi(z)))$, $8M_2(z,\Phi(z))$ all vanish modulo 16, also $P_4(z,\Phi(z))$ must have this property; but this means that $g_1(z)$ and $g_0(z)$ both vanish modulo 16.

If we combine (D.2), (D.4), (D.5), (D.6), then we obtain our claim. □

Now we put ourselves in the situation that we want to describe the coefficients of the formal power series $F(z)$ modulo 16, where $F(z)$ solves a Riccati-type differential equation of the form (4.1), and that we try to solve this problem by expressing $F(z)$ in the form

$$F(z) = \sum_{i=0}^{5} a_i(z)\Phi^i(z) \quad \text{modulo 16},$$

where the $a_i(z)$'s are Laurent polynomials in z over the integers to be determined. Let us assume that, while following the approach outlined in Section 4 (with $M_{16}(z,\Phi(z))$ in place of the polynomial in (4.4)), we have already reached the level of modulus 8, that is, that we have found Laurent polynomials $a_{0,3}(z), a_{1,3}(z), a_{2,3}(z), a_{3,3}(z), a_{4,3}(z), a_{5,3}(z)$ such that

$$\sum_{i=0}^{5} a_{i,3}(z)\Phi^i(z)$$

solves the differential equation (4.1) modulo 8. According to the Ansatz (4.6)–(4.8) with $\beta = 3$, we now substitute

$$\sum_{i=0}^{5} (a_{i,3}(z) + 8b_{i,4}(z))\Phi^i(z) \quad \text{(D.7)}$$

(where the $b_{i,4}(z)$'s are at this point undetermined Laurent polynomials in z) instead of $F(z)$ in (4.1). For the sake of better readability, in the sequel we write $b_0(z)$ for $b_{0,4}(z)$, etc. After simplification of the left-hand side of (4.1) modulo 16 as described below (4.8), and after reduction of the resulting expression modulo $M_{16}(z,\Phi(z))$ (which is a polynomial in $\Phi(z)$ of degree 6), we obtain a polynomial of the form

$$8\sum_{i=0}^{5} \Big(p_i(z) + G_i\big(z,\mathbf{b}(z),\mathbf{b}'(z)\big)\Big)\Phi^i(z), \quad \text{(D.8)}$$

where the $p_i(z)$'s are certain Laurent polynomials in z over the integers, and the $G_i\big(z, \mathbf{b}(z), \mathbf{b}'(z)\big)$'s are certain linear forms in

$$b_0(z), b_1(z), b_2(z), b_3(z), b_4(z), b_5(z) \text{ and } b'_0(z), b'_1(z), b'_2(z), b'_3(z), b'_4(z), b'_5(z),$$

with coefficients that are (known) Laurent polynomials in z over the integers.

Our goal is to find Laurent polynomials $b_0(z), b_1(z), b_2(z), b_3(z), b_4(z), b_5(z)$ such that the expression (D.8) is zero modulo 16 as Laurent series in z. Lemma 39, combined with the explicit forms of $M_2(z,t)$ and $M_8(z,t)$ given in Proposition 2, then says that

$$\begin{aligned}
8\Big(p_0(z) + G_0\big(z, \mathbf{b}(z), \mathbf{b}'(z)\big)\Big) &= (4z + 10z^2)c_3(z) + 8zc_5(z) \quad \text{modulo } 16,\\
8\Big(p_1(z) + G_1\big(z, \mathbf{b}(z), \mathbf{b}'(z)\big)\Big) &= (4z + 10z^2)c_2(z) + (12 + 4z)c_3(z) + 8zc_4(z) + 8c_5(z)\\
&\qquad\qquad \text{modulo } 16,\\
8\Big(p_2(z) + G_2\big(z, \mathbf{b}(z), \mathbf{b}'(z)\big)\Big) &= (12 + 4z)c_2(z) + (6 + 4z)c_3(z) + 8c_4(z) + 8c_5(z)\\
&\qquad\qquad \text{modulo } 16,\\
8\Big(p_3(z) + G_3\big(z, \mathbf{b}(z), \mathbf{b}'(z)\big)\Big) &= (6 + 4z)c_2(z) + 12c_3(z) + 8c_4(z) \quad \text{modulo } 16,\\
8\Big(p_4(z) + G_4\big(z, \mathbf{b}(z), \mathbf{b}'(z)\big)\Big) &= 12c_2(z) + 2c_3(z) \quad \text{modulo } 16,\\
8\Big(p_5(z) + G_5\big(z, \mathbf{b}(z), \mathbf{b}'(z)\big)\Big) &= 2c_2(z) \quad \text{modulo } 16,
\end{aligned}$$

for suitable Laurent polynomials $c_2(z), c_3(z), c_4(z), c_5(z)$. From the last congruence one sees that $c_2(z)$ is actually zero modulo 4, and then the next-to-last congruence implies that the same holds for $c_3(z)$. Writing $4a(z) = c_2(z)$, $4b(z) = c_3(z)$, $c(z) = c_4(z)$, $d(z) = c_5(z)$, we see that the above system of congruences simplifies to

$$\begin{aligned}
G_0\big(z, \mathbf{b}(z), \mathbf{b}'(z)\big) &= p_0(z) + z^2 b(z) + zd(z) \quad \text{modulo } 2,\\
G_1\big(z, \mathbf{b}(z), \mathbf{b}'(z)\big) &= p_1(z) + z^2 a(z) + zc(z) + d(z) \quad \text{modulo } 2,\\
G_2\big(z, \mathbf{b}(z), \mathbf{b}'(z)\big) &= p_2(z) + b(z) + c(z) + d(z) \quad \text{modulo } 2,\\
G_3\big(z, \mathbf{b}(z), \mathbf{b}'(z)\big) &= p_3(z) + a(z) + c(z) \quad \text{modulo } 2,\\
G_4\big(z, \mathbf{b}(z), \mathbf{b}'(z)\big) &= p_4(z) + b(z) \quad \text{modulo } 2,\\
G_5\big(z, \mathbf{b}(z), \mathbf{b}'(z)\big) &= p_5(z) + a(z) \quad \text{modulo } 2.
\end{aligned} \tag{D.9}$$

This puts us in the situation of Lemma 12, except that on the right-hand sides of the congruences (denoted by $r_i(z)$, $i = 1, 2, \ldots, N$, in Lemma 12) there appear the unknown Laurent polynomials $a(z), b(z), c(z), d(z)$. Still, the idea of the proof of Lemma 12 may be applied: the system of congruences (D.9) can be solved with respect to the "variables" $b_0(z), b_1(z), b_2(z), b_3(z), b_4(z), b_5(z)$ by separating odd and even parts, and thereby converting the original system (4.9) of congruences into the system (4.10) of linear congruences for the odd and even parts of the variables. We solve this last system over the

field of *rational* functions over $\mathbb{Z}/2\mathbb{Z}$, where odd and even parts of the "auxiliary variables" $a(z), b(z), c(z), d(z)$ "sit" inside the odd and even parts of the "constants" $r_i(z)$. In the end, if odd and even parts of the variables $b_0(z), b_1(z), b_2(z), b_3(z), b_4(z), b_5(z)$ are put together, then we are able to express these variables in the form

$$b_i(z) = \frac{q_i(z) + H_i\big(z, a^{(o)}(z), a^{(e)}(z), \ldots, d^{(o)}(z), d^{(e)}(z)\big)}{P(z)} \quad \text{modulo } 2, \qquad i = 0, 1, \ldots, 5, \tag{D.10}$$

where the $q_i(z)$'s are (known) Laurent polynomials in z over the integers, $P(z)$ is a (known) polynomial in z over the integers, and the

$$H_i\big(z, a^{(o)}(z), a^{(e)}(z), \ldots, d^{(o)}(z), d^{(e)}(z)\big)\text{'s}$$

are linear forms in $a^{(o)}(z), a^{(e)}(z), \ldots, d^{(o)}(z), d^{(e)}(z)$ with coefficients that are (known) Laurent polynomials in z over the integers.

The task now is to choose $a^{(o)}(z), a^{(e)}(z), \ldots, d^{(o)}(z), d^{(e)}(z)$ in such a way that in each of the fractions on the right-hand sides of (D.10) the denominator $P(z)$ cancels out.

In order to carry out this task, we decompose $P(z)$ into its prime factors (over $\mathbb{Z}/2\mathbb{Z}$), say

$$P(z) = \prod_{j=1}^{\ell} P_j^{m_j}(z) \quad \text{modulo } 2.$$

Using a standard inductive procedure,[16] we find $a^{(o)}(z), a^{(e)}(z), \ldots, d^{(o)}(z), d^{(e)}(z)$ (if there are) such that

$$q_i(z) + H_i\big(z, a^{(o)}(z), a^{(e)}(z), \ldots, d^{(o)}(z), d^{(e)}(z)\big) = 0 \pmod{P_j^{m_j}(z)}, \qquad i = 0, 1, \ldots, 5,\ j = 1, 2, \ldots, \ell, \tag{D.11}$$

(again, over the field $\mathbb{Z}/2\mathbb{Z}$), and then put the particular results for each j together by means of the Chinese remainder theorem. We only discuss the generic case here, the discussion for other cases being completely analogous. Namely, generically, having to solve 6 equations in 8 variables, one will be able to express six of the variables in terms of two "free" variables. Let us say, $b^{(o)}(z), b^{(e)}(z), c^{(o)}(z), c^{(e)}(z), d^{(o)}(z), d^{(e)}(z)$ can be

[16] One first solves (D.11) modulo $P_j(z)$ (instead of $P_j^{m_j}(z)$); this means solving a system of linear equations over a field. If one has solved (D.11) already modulo $P_j^h(z)$, for each variable $\mathrm{var}(z)$ one makes the Ansatz $\mathrm{var}(z) = \mathrm{var}_0(z) + \mathrm{var}_1(z)P_j^h(z)$, where $\mathrm{var}_0(z)$ is the value of $\mathrm{var}(z)$ in the solution modulo $P_j^h(z)$. If this is substituted in (D.11), after cancellation, solving (D.11) modulo $P_j^{h+1}(z)$ boils again down to solving a system of linear equations modulo $P_j(z)$, that is, over a field.

expressed in terms of $a^{(o)}(z), a^{(e)}(z)$,

$$\begin{aligned}
b^{(o)}(z) &= s_1(z) + u_1(z)a^{(o)}(z) + v_1(z)a^{(e)}(z) \quad \text{modulo 2,}\\
b^{(e)}(z) &= s_2(z) + u_2(z)a^{(o)}(z) + v_2(z)a^{(e)}(z), \quad \text{modulo 2,}\\
c^{(o)}(z) &= s_3(z) + u_3(z)a^{(o)}(z) + v_3(z)a^{(e)}(z), \quad \text{modulo 2,}\\
c^{(e)}(z) &= s_4(z) + u_4(z)a^{(o)}(z) + v_4(z)a^{(e)}(z), \quad \text{modulo 2,}\\
d^{(o)}(z) &= s_5(z) + u_5(z)a^{(o)}(z) + v_5(z)a^{(e)}(z), \quad \text{modulo 2,}\\
d^{(e)}(z) &= s_6(z) + u_6(z)a^{(o)}(z) + v_6(z)a^{(e)}(z) \quad \text{modulo 2,}
\end{aligned} \tag{D.12}$$

where the $s_i(z)$'s, the $u_i(z)$'s, and the $v_i(z)$'s are certain (known) Laurent polynomials in z over the integers, and where we are free to choose $a^{(o)}(z)$ and $a^{(e)}(z)$. If this is substituted in (D.10), then on the right-hand sides the denominator $P(z)$ cancels out, and $b_0(z), b_1(z), b_2(z), b_3(z), b_4(z), b_5(z)$ will all be equal to Laurent polynomials in z over the integers.

We are still not finished, though. In the "solution" (D.12) the Laurent polynomials $a^{(o)}(z), b^{(o)}(z), c^{(o)}(z), d^{(o)}(z)$ must be chosen as odd, while the Laurent polynomials $a^{(e)}(z), b^{(e)}(z), c^{(e)}(z), d^{(e)}(z)$ must be chosen as even. In order to achieve this, we must (again) separate odd and even parts: doing so in (D.12) yields the system

$$\begin{aligned}
0 &= s_1^{(e)}(z) + u_1^{(o)}(z)a^{(o)}(z) + v_1^{(e)}(z)a^{(e)}(z) \quad \text{modulo 2,}\\
0 &= s_2^{(o)}(z) + u_2^{(e)}(z)a^{(o)}(z) + v_2^{(o)}(z)a^{(e)}(z), \quad \text{modulo 2,}\\
0 &= s_3^{(e)}(z) + u_3^{(o)}(z)a^{(o)}(z) + v_3(e)(z)a^{(e)}(z), \quad \text{modulo 2,}\\
0 &= s_4^{(o)}(z) + u_4^{(e)}(z)a^{(o)}(z) + v_4^{(o)}(z)a^{(e)}(z), \quad \text{modulo 2,}\\
0 &= s_5^{(e)}(z) + u_5^{(o)}(z)a^{(o)}(z) + v_5^{(e)}(z)a^{(e)}(z), \quad \text{modulo 2,}\\
0 &= s_6^{(o)}(z) + u_6^{(e)}(z)a^{(o)}(z) + v_6^{(o)}(z)a^{(e)}(z) \quad \text{modulo 2.}
\end{aligned} \tag{D.13}$$

This is a system of six linear congruences with two variables, $a^{(o)}(z)$ and $a^{(e)}(z)$, where the first of these should be an odd Laurent polynomial and the second an even one. It is of the type of the system of congruences (4.10). How to solve such a system is explained in the paragraph below the proof of Lemma 12. (One first solves over the field of rational functions in z over $\mathbb{Z}/2\mathbb{Z}$, and then cancels denominators, if possible.) Moreover, the argument in the proof of Lemma 12 showing that, if (4.10) has *some* solution in Laurent polynomials, then it also has a solution in which all $f_j^{(1)}(z)$'s are even Laurent polynomials and all $f_j^{(2)}(z)$'s are odd Laurent polynomials, also applies to the system (D.13) to guarantee that, if one is able to find *some* solution $a^{(o)}(z), a^{(e)}(z)$, then one can also find one in which $a^{(o)}(z)$ is an odd Laurent polynomial and $a^{(e)}(z)$ is an even Laurent polynomial.

If one is able to carry through this procedure, then one has found the unknowns $b_{i,4}(z)$, $i = 0, 1, \ldots, 5$, so that (D.7) produces the desired description modulo 16 of the solution $F(z)$ to the Riccati-type differential equation (4.1). Conversely, if one of the systems

of linear congruences which one has to solve along the way (these are (D.9), (D.11), and (D.13)) has no solution, then one has *proved* that it is impossible to describe the series $F(z)$ modulo 16 in terms of a polynomial in $\Phi(z)$ with coefficients that are Laurent polynomials in z over the integers.

References

[1] S. A. Abramov and M. van Hoeij, Desingularization of linear difference operators with polynomial coefficients, *Proc. ISSAC'99*, pp. 269–275, 1999.

[2] D. Armstrong, *Generalized noncrossing partitions and combinatorics of Coxeter groups*, Mem. Amer. Math. Soc., vol. 202, no. 949, Amer. Math. Soc., Providence, R.I., 2009.

[3] P. J. Cameron and T. W. Müller, A descent principle in modular subgroup arithmetic, *J. Pure Appl. Algebra* **203** (2005), 189–203.

[4] F. Chyzak, *Fonctions holonomes en calcul formel*, Ph.D. thesis, École polytechnique, Paris, 1998.

[5] F. Chyzak and B. Salvy, Non-commutative elimination in Ore algebras proves multivariate holonomic identities, *J. Symbolic Comput.* **26** (1998), 187–227.

[6] L. Comtet, *Advanced Combinatorics*, D. Reidel, Dordrecht, Holland, 1974.

[7] A. D. D. Craik, Prehistory of Faà di Bruno's formula, *Amer. Math. Monthly* **112** (2005), 119–130.

[8] K. S. Davis and W. A. Webb, Lucas' theorem for prime powers, Europ. J. Combin. **11** (1990), 229–233.

[9] I. M. S. Dey, Schreier systems in free products, *Proc. Glasgow Math. Soc.* **7** (1965), 61–79.

[10] A. Dress and T. W. Müller, Decomposable functors and the exponential principle, *Adv. in Math.* **129** (1997), 188–221.

[11] S.-P. Eu, S.-C. Liu and Y.-N. Yeh, Catalan and Motzkin numbers modulo 4 and 8, *Europ. J. Combin.* **29** (2008), 1449–1466.

[12] G. Frobenius, Verallgemeinerung des Sylow'schen Satzes, *Sitz.ber. Königl. Preuss. Akad. Wiss. Berlin* (1895), 981–993.

[13] G. Frobenius, Über einen Fundamentalsatz der Gruppentheorie, *Sitz.ber. Königl. Preuss. Akad. Wiss. Berlin* **44** (1903), 987–991.

[14] C. Godsil, W. Imrich, and R. Razen, On the number of subgroups of given index in the modular group, *Monatsh. Math.* **87** (1979), 273–280.

[15] A. Granville, Arithmetic properties of binomial coefficients, I: Binomial coefficients modulo prime powers, in: Organic mathematics (Burnaby, BC, 1995), CMS Conf. Proc., vol. 20, Amer. Math. Soc., Providence, RI, 1997, pp. 253–276.

[16] M. Kauers, Guess, *Mathematica* package available at
`http://www.risc.jku.at/research/combinat/software/Guess`.

[17] P. Hall, On a theorem of Frobenius, *Proc. London Math. Soc.* (2) **40** (1935), 468–501.

[18] W. P. Johnson, The curious history of Faà di Bruno's formula, *Amer. Math. Monthly* **109** (2002), 217–234.

[19] C. Koutschan, *Advanced applications of the holonomic systems approach*, RISC, J. Kepler University, Linz, Ph.D. thesis, 2009; *Mathematica* implementation available at `http://www.risc.jku.at/research/combinat/software/HolonomicFunctions`.

[20] C. Krattenthaler and T. W. Müller, Parity patterns associated with lifts of Hecke groups, *Abh. Math. Sem. Univ. Hamburg* **78** (2008), 99–147.

[21] A. M. Legendre, *Essai sur la théorie des nombres*, 2ed., Courcier, Paris, 1808.

[22] S.-C. Liu and J. C.-C. Yeh, Catalan numbers modulo 2^k, *J. Integer Sequences* **13** (2010), Art. 10.5.4, 26 pages.

[23] C. Mallinger, *Algorithmic manipulations and transformations of univariate holonomic functions and sequences*, diploma thesis, RISC, J. Kepler University, Linz, 1996; *Mathematica* implementation available at
`http://www.risc.jku.at/research/combinat/software/GeneratingFunctions`.

[24] T. W. Müller, Combinatorial aspects of finitely generated virtually free groups, *J. London Math. Soc.* (2) **44** (1991), 75–94.

[25] T. W. Müller, Modular subgroup arithmetic and a theorem of Philip Hall, *Bull. London Math. Soc.* **34** (2002), 587–598.

[26] T. W. Müller, Modular subgroup arithmetic in free products, *Forum Math.* **15** (2003), 759–810.

[27] T. W. Müller, Parity patterns in Hecke groups and Fermat primes. In: *Groups: Topological, Combinatorial, and Arithmetic Aspects,* Proceedings of a conference held 1999 in Bielefeld (T. W. Müller, ed.), LMS Lecture Note Series vol. 311, Cambridge University Press, Cambridge, 2004, 327–374.

[28] T. W. Müller and J.-C. Schlage-Puchta, Modular arithmetic of free subgroups, *Forum Math.* **17** (2005), 375–405.

[29] T. W. Müller and J.-C. Schlage-Puchta, Divisibility properties of subgroup numbers for the modular group, *New York J. Math.* **11** (2005), 205–224.

[30] A. Postnikov and B. E. Sagan, What power of two divides a weighted Catalan number?, *J. Combin. Theory Ser. A* **114** (2007), 970–977.

[31] B. Salvy and P. Zimmermann, Gfun: a Maple package for the manipulation of generating and holonomic functions in one variable, *ACM Trans. Math. Software* **20** (1994); available as part of the standard distribution of *Maple*.

[32] R. P. Stanley, *Enumerative Combinatorics*, vol. 2, Cambridge University Press, Cambridge, 1999.

[33] R. P. Stanley, *Catalan Addendum*, continuation of Exercise 6.19 from [32]; available at `http://math.mit.edu/~rstan/ec/catadd.pdf`.

[34] W. Stothers, The number of subgroups of given index in the modular group, *Proc. Royal Soc. Edinburgh, Sec. A* **78** (1977), 105–112.

[35] L. Sylow, Théorèmes sur les groupes de substitutions, *Math. Ann.* **5** (1872), 584–594.

[36] H. S. Wilf, *generatingfunctionology*, 2nd edition, Academic Press, San Diego, 1994.

[37] H. S. Wilf and D. Zeilberger, An algorithmic proof theory for hypergeometric (ordinary and "q") multisum/integral identities, *Invent. Math.* **108** (1992), 575–633.

[38] G. Xin and J.-F. Xu, A short approach to Catalan numbers modulo 2^r, Electron. J. Combin. **18**(1) (2011), Article #P177, 12 pp.

[39] D. Zeilberger, A holonomic systems approach to special functions identities, *J. Comput. Appl. Math.* **32** (1990), 321–368.