A RICCATI DIFFERENTIAL EQUATION AND FREE SUBGROUP NUMBERS FOR LIFTS OF $\mathrm{PSL}_2(\mathbb{Z})$ MODULO PRIME POWERS

C. KRATTENTHALER† AND T. W. MÜLLER*

Abstract. It is shown that the number f_λ of free subgroups of index 6λ in the modular group $\mathrm{PSL}_2(\mathbb{Z})$, when considered modulo a prime power p^α with $p \ge 5$, is always (ultimately) periodic. In fact, an analogous result is established for a one-parameter family of lifts of the modular group (containing $\mathrm{PSL}_2(\mathbb{Z})$ as a special case), and for a one-parameter family of lifts of the Hecke group $\mathfrak{H}(4) = C_2 * C_4$. All this is achieved by explicitly determining Padé approximants to solutions of a certain multi-parameter family of Riccati differential equations. Our main results complement previous work by Kauers and the authors ([*Electron. J. Combin.* **18**(2) (2012), Article P37] and [*"A method for determining the mod-3^k behaviour of recursive sequences"*, preprint]), where it is shown, among other things, that the free subgroup numbers of $\mathrm{PSL}_2(\mathbb{Z})$ and its lifts display rather complex behaviour modulo powers of 2 and 3.

1. Introduction

Beginning with the work of Sylow [26], Frobenius [5], [6], and P. Hall [9], [10], the study of congruences for subgroup numbers and related invariants has played an important rôle in group theory. Over the last fifteen years, there has been active interest in divisibility properties of subgroup numbers of (finitely generated) infinite groups; these may, to some extent, be seen as analogues of classical results for finite groups. The systematic study of the subgroup arithmetic of infinite groups begins with [18], which investigates the parity of subgroup numbers and free subgroup numbers in arbitrary Hecke groups $\mathfrak{H}(q) = C_2 * C_q$ with $q \ge 3$.[1] The results of [18] were subsequently generalised to larger classes of groups and arbitrary prime modules in [4], [14], [19], [20], [21], and [22].

A first attempt at obtaining congruences modulo higher prime powers was made in [22], which studies the subgroup numbers of the inhomogeneous modular group $\mathfrak{H}(3) \cong \mathrm{PSL}_2(\mathbb{Z})$ modulo 8, and derives a congruence modulo 16 for the number of free subgroups in $\mathrm{PSL}_2(\mathbb{Z})$ of given finite index. The real breakthrough concerning this kind of problem however occurred in the recent papers [12] and [15], which introduce a method leading to semi-automatic existence proofs as well as explicit computation of such congruences modulo 2-powers and 3-powers for a wide variety of combinatorial sequences. Among

2010 *Mathematics Subject Classification.* Primary 05A15; Secondary 05E99 11A07 20E06 20E07 68W30.

Key words and phrases. Polynomial recurrences, free subgroup numbers, inhomogeneous modular group, Padé approximant, hypergeometric series.

†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] This paper circulated in the community since 1998 before finally appearing in print in 2004.

other things, this novel approach leads to congruences modulo arbitrary 2-powers for the number $f_\lambda(m)$ of free subgroups of index $6m\lambda$ in lifts $\Gamma_m(3)$ of $\mathrm{PSL}_2(\mathbb{Z})$ of the form

$$\Gamma_m(3) = C_{2m} \underset{C_m}{*} C_{3m} = \left\langle x, y \,\middle|\, x^{2m} = y^{3m} = 1,\ x^2 = y^3 \right\rangle, \quad m \ge 1; \tag{1.1}$$

see Theorems 19 and 20 in [12]. The method developed in [12] can in principle be adapted to yield congruences modulo other prime powers p^α, and this has been carried out in detail in [15] for $p = 3$. Among many other results, we obtain there congruences for the function $f_\lambda(m)$ modulo arbitrary 3-powers; cf. Section 16 in [15]. The congruences obtained in this way for $f_\lambda(m)$ show a highly non-trivial behaviour of these sequences modulo 2-powers and 3-powers. For instance, for the sequence $f_\lambda = f_\lambda(1)$ of free subgroup numbers of the group $\mathrm{PSL}_2(\mathbb{Z})$, one can show that:

(1) $f_\lambda \equiv -1 \pmod 3$ if, and only if, the 3-adic expansion of λ is an element of $\{0,2\}^*1$;

(2) $f_\lambda \equiv 1 \pmod 3$ if, and only if, the 3-adic expansion of λ is an element of

$$\{0,2\}^*100^* \cup \{0,2\}^*122^*;$$

(3) for all other λ, we have $f_\lambda \equiv 0 \pmod 3$;

cf. [15, Cor. 53]. Here, for a set Ω, we denote by Ω^* the free monoid generated by Ω.

The general theory of finitely generated virtually free groups implies that the generating function for the free subgroup numbers $f_\lambda(m)$ satisfies a Riccati differential equation, see (4.1). This theory might also lead one to suspect that the primes 2 and 3 should be special in this context. One of the main results of the present paper confirms this conjecture in a strong and surprising form. Namely, we show the following.

Theorem. *Let m be a positive integer, p a prime number with $p \ge 5$, and let α be a positive integer. Then the generating function $F_m(z) = 1 + \sum_{\lambda\ge1} f_\lambda(m) z^\lambda$, when coefficients are reduced modulo p^α, can be represented as a rational function. Equivalently, the sequence $(f_\lambda(m))_{\lambda\ge1}$ is ultimately periodic modulo p^α.*

This is Theorem 8 in Section 4. The proof relies on finding an explicit approximate rational solution for a relevant multi-parameter class of Riccati differential equations; see Theorem 1 in the next section. In fact, this theorem implies a formula in terms of an explicit rational function for the generating function $F_m(z)$ when coefficients are reduced modulo p; see the proof of Theorem 8 in Section 4. A more detailed p-adic analysis of the expressions extracted from Theorem 1 allows us to derive even more precise results on the form of the rational functions and on the period lengths of the sequence $(f_\lambda(m))_{\lambda\ge1}$ modulo concrete prime powers p^α; see Section 5. Moreover, Theorem 1 is general enough to also produce analogous results for the free subgroup numbers of lifts of the Hecke group $\mathfrak{H}(4)$; see Section 6.

The proof of Theorem 1 occupies Section 3. Section 4 presents the (very short) derivation of the theorem above from Theorem 1. As already said, Section 5 establishes more precise results for the subgroup numbers $f_\lambda(m)$. More specifically, Theorem 11 identifies the denominators of the rational functions which one obtains when the coefficients of the generating function $1 + \sum_{\lambda\ge1} f_\lambda(m) z^\lambda$ are reduced modulo a prime power p^α with $p \ge 5$. Theorems 12–17 then illustrate this general result for the numbers $f_\lambda = f_\lambda(1)$ (i.e., the free subgroup numbers of the modular group $\mathrm{PSL}_2(\mathbb{Z})$ itself) when reduced modulo the primes $p = 7, 11, 13$. In particular, the exact minimal period is determined in these cases. Section 6 presents the analogous results for the free subgroup numbers of the lifts of $\mathfrak{H}(4)$. Finally, the rather interesting and involved way which led us to conjecture formulae (2.3) and (2.4) for numerator and denominator of the approximate rational solution $R_n(z)$ of the differential equation (2.1) (which is the subject of Theorem 1) is explained in an appendix.

Note. This paper is accompanied by two *Mathematica* files that allow an interested reader to compute the rational functions representing the reductions modulo p^α of the generating function $1+\sum_{\lambda\ge1} f_\lambda z^\lambda$ for the number f_λ of free subgroups of index 6λ in $\mathrm{PSL}_2(\mathbb{Z})$ and of the generating function $1+\sum_{\lambda\ge1} f_\lambda^{(4)} z^\lambda$ for the number $f_\lambda^{(4)}$ of free subgroups of index 4λ in $\mathfrak{H}(4)$. The result is given as partial fraction expansion of the form predicted by Theorems 11 and 21, respectively. The files are available at the article's website `http://www.mat.univie.ac.at/~kratt/artikel/psl2zmod.html`.

2. Approximate rational solutions for a Riccati differential equation

We consider the Riccati differential equation

$$(1-Az)F(z)-Bz^2F'(z)-CzF^2(z)-1-Dz=0, \tag{2.1}$$

where A,B,C,D are constants. The technical main result of our paper is the following.

Theorem 1. *For every positive integer n, there exist uniquely determined polynomials $P_n(z)=1+\sum_{k=1}^n p_{n,k}z^k$ and $Q_n(z)=1+\sum_{k=1}^n q_{n,k}z^k$, where $p_{n,k}$ and $q_{n,k}$ are homogeneous polynomials in A,B,C,D of degree k over the integers, such that the rational function $R_n(z)=P_n(z)/Q_n(z)$ satisfies the differential equation*

$$\begin{aligned}(1-Az)&R_n(z)-Bz^2R_n'(z)-CzR_n^2(z)-1-Dz\\ &=-\frac{z^{2n+1}}{Q_n^2(z)}(A+C+D)\prod_{\ell=1}^n(\ell AB+AC+CD+\ell^2B^2+2\ell BC+C^2).\end{aligned} \tag{2.2}$$

Moreover, the coefficients $p_{n,k}$ and $q_{n,k}$ are given explicitly by

$$\begin{aligned}p_{n,n-k}=&\frac{(-1)^{n+1}B^{n-k}}{2C\,(\frac{E}{B}-k)_{2k+1}}\\ &\times\Bigg(\big(\tfrac{A+2C+E}{2B}\big)_{n+1}\sum_{j=0}^k\binom{k+j}{k}\binom{n-j}{k-j}\big(-\tfrac{E}{B}+j+1\big)_{k-j}\big(\tfrac{A+2C-E}{2B}\big)_j\\ &\qquad\cdot\big(A+\tfrac{2kj}{k+j}B-\tfrac{k-j}{k+j}E\big)\\ &-\big(\tfrac{A+2C-E}{2B}\big)_{n+1}\sum_{j=0}^k\binom{k+j}{k}\binom{n-j}{k-j}\big(\tfrac{E}{B}+j+1\big)_{k-j}\big(\tfrac{A+2C+E}{2B}\big)_j\\ &\qquad\cdot\big(A+\tfrac{2kj}{k+j}B+\tfrac{k-j}{k+j}E\big)\Bigg)\end{aligned} \tag{2.3}$$

and

$$q_{n,n-k}=\frac{(-1)^nB^{n-k}}{(\frac{E}{B}-k)_{2k+1}}$$
$$\times\Bigg(\left(\tfrac{A+2C+E}{2B}\right)_{n+1}\sum_{j=0}^{k}\binom{k+j}{k}\binom{n-j}{k-j}\left(-\tfrac{E}{B}+j+1\right)_{k-j}\left(\tfrac{A+2C-E}{2B}\right)_j$$
$$-\left(\tfrac{A+2C-E}{2B}\right)_{n+1}\sum_{j=0}^{k}\binom{k+j}{k}\binom{n-j}{k-j}\left(\tfrac{E}{B}+j+1\right)_{k-j}\left(\tfrac{A+2C+E}{2B}\right)_j\Bigg),\tag{2.4}$$

where $E^2=A^2-4CD$, *and the* Pochhammer symbol $(\alpha)_m$ *is defined by* $(\alpha)_m=\alpha(\alpha+1)(\alpha+2)\cdots(\alpha+m-1)$ *for* $m>0$, *and* $(\alpha)_0=1$.

Remark 2. (1) In the sums in (2.3) it might seem that there is a problem if $k=j=0$. The correct way to interpret (2.3) for $k=0$ is the following: one first leaves k undetermined; then there is no problem to calculate the expression $A+\frac{2kj}{k+j}B-\frac{k-j}{k+j}E$ when $j=0$, it simply equals $A-E$. Subsequently, one can safely set $k=0$. A similar remark applies to its "companion expression" in the second sum. So, explicitly,

$$p_{n,n}=\frac{(-1)^{n+1}B^{n+1}}{2CE}\Big((A-E)\left(\tfrac{A+2C+E}{2B}\right)_{n+1}-(A+E)\left(\tfrac{A+2C-E}{2B}\right)_{n+1}\Big).\tag{2.5}$$

(2) The rational function solutions $R_n(z)$ for $n=1,2,3$ are displayed in the appendix as (A.2)–(A.4).

(3) Formulae for the first few coefficients $p_{n,k}$ and $q_{n,k}$, $k=1,2,3$, are displayed in (A.5)–(A.10) in the appendix. Assuming Theorem 1, these (originally experimentally found) formulae can be established as follows: according to the theorem, the coefficients $p_{n,k}$ and $q_{n,k}$ are in particular polynomials in A of degree at most k. As such, they are uniquely determined by $k+1$ special evaluations. These can be found from Formulae (2.3) and (2.4) by setting $A=-2C-E-2Bs$, $s=0,1,\dots,k$. Indeed, with these specialisations, the term $\left(\frac{A+2C+E}{2B}\right)_{n+1}$ vanishes for $n\ge k$, so that the first terms between parentheses in (2.3) and (2.4) vanish. For the same reason, the term $\left(\frac{A+2C+E}{2B}\right)_j$ in the second sums over j in (2.3) and (2.4) vanishes for $j\ge k+1$, so that only the terms for $j=0,1,\dots,k$ remain.

(4) It is easy to see that $R_n(z)$ solves (2.2) if, and only if, $R_n(z/B)$ solves (2.2) with B replaced by 1, A replaced by A/B, C replaced by C/B, and D replaced by D/B. Hence, it suffices to consider the special case where $B=1$. We shall occasionally make use of this simplification of the problem.

(5) It is in fact not necessary to specify the precise form of the right-hand side in (2.2) once we know that it is of the form $\mathcal{O}(z^{2n+1})$, that is, a formal power series of order at least $2n+1$; see Remark 5. Consequently, a different way to view the rational function $R_n(z)$ is as the *Padé approximant* of order n to the solution of the Riccati differential equation (2.1). See also the proof of Lemma 4.

3. Proof of Theorem 1

The proof of Theorem 1 is accomplished by dividing the assertion of the theorem into several parts, and then treating each of these partial assertions in a separate lemma. More precisely, in Lemma 3 below we show that the rational function $R_n(z) = P_n(z)/Q_n(z)$ given by (2.3) and (2.4) does indeed satisfy the differential equation (2.2), while uniqueness of solution is the subject of Lemma 4. The fact that the coefficients $p_{n,k}$ and $q_{n,k}$ in (2.3) and (2.4) are homogeneous polynomials in A, B, C, D of degree k is then established in Lemma 6, while integrality of their coefficients is proved in Lemma 7. Taken together, these lemmas provide a full proof of Theorem 1.

Lemma 3. *The rational function $R_n(z) = P_n(z)/Q_n(z)$, with the coefficients of the polynomials $P_n(z)$ and $Q_n(z)$ given by* (2.3) *and* (2.4), *satisfies the differential equation* (2.2).

Proof. If we substitute $R_n(z) = P_n(z)/Q_n(z)$ into the differential equation and multiply both sides by $Q_n^2(z)$, then we see that, in order to establish the lemma, we have to demonstrate the equation

$$(1 - Az)P_n(z)Q_n(z) - Bz^2(P_n'(z)Q_n(z) - P_n(z)Q_n'(z)) - CzP_n^2(z) - (1 + Dz)Q_n^2(z)$$
$$= -z^{2n+1}(A + C + D)\prod_{\ell=1}^{n}(\ell AB + AC + CD + \ell^2 B^2 + 2\ell BC + C^2). \quad (3.1)$$

We start by verifying that the coefficients of z^{2n+1} on both sides of (3.1) agree. For the sake of better readability, let us write

$$\Pi_+ := B^{n+1}\left(\tfrac{A+2C+E}{2B}\right)_{n+1} \quad \text{and} \quad \Pi_- := B^{n+1}\left(\tfrac{A+2C-E}{2B}\right)_{n+1}. \quad (3.2)$$

Using this notation plus (2.5), the coefficient $p_{n,n}$ is seen to be given by

$$p_{n,n} = \frac{(-1)^{n+1}}{2CE}\big((A - E)\Pi_+ - (A + E)\Pi_-\big), \quad (3.3)$$

while, by (2.4), the coefficient $q_{n,n}$ is given by

$$q_{n,n} = \frac{(-1)^n}{E}\big(\Pi_+ - \Pi_-\big). \quad (3.4)$$

Consequently, the coefficient of z^{2n+1} on the left-hand side of (3.1) equals

$$\begin{aligned}-Ap_{n,n}q_{n,n} - Cp_{n,n}^2 - Dq_{n,n}^2 &= \frac{1}{4C^2E^2}\Big(\big(A(A - E)(2C) - C(A - E)^2 - D(2C)^2\big)\Pi_+^2\\ &\quad + \big(-2A^2(2C) + 2C(A^2 - E^2) + 2D(2C)^2\big)\Pi_+\Pi_-\\ &\quad + \big(A(A + E)(2C) - C(A + E)^2 - D(2C)^2\big)\Pi_-^2\Big)\\ &= -\frac{1}{C}\Pi_+\Pi_-,\end{aligned}$$

where we have used the relation $E^2 = A^2 - 4CD$ in the last step. It is straightforward to see that this is identical with the coefficient of z^{2n+1} on the right-hand side of (3.1).

We now divide both sides of (3.1) by z^{2n+1}, then differentiate them with respect to z, and finally multiply both sides of the resulting equation by z^{2n+2}. In this way, we obtain the equation

$$\begin{aligned}P_n(z)\big(2CnzP_n(z) - 2Cz^2P_n'(z) - (2n+1)Q_n(z) + zQ_n'(z)\\ - z^2(A+2Bn-B)Q_n'(z) + 2AnzQ_n(z) + Bz^3Q_n''(z)\big)\\ + Q_n(z)\big(zP_n'(z) - z^2(A-2Bn+B)P_n'(z) - Bz^3P_n''(z)\\ + (2n+1)Q_n(z) + 2DnzQ_n(z) - 2Dz^2Q_n'(z) - 2zQ_n'(z)\big) = 0. \quad (3.5)\end{aligned}$$

Since we already know that the coefficients of z^{2n+1} on both sides of (3.1) agree, establishing (3.5) is completely equivalent to establishing (3.1). We concentrate on the former task from now on.

The crucial observation is that, if (3.5) is to hold, then the first factor between parentheses in (3.5) must be a (polynomial) multiple of $Q_n(z)$, while the second factor between parentheses must be a multiple of $P_n(z)$. Indeed, our claim is that

$$\begin{aligned}2CnzP_n(z) - 2Cz^2P_n'(z) - (2n+1)Q_n(z) + zQ_n'(z) - z^2(A+2Bn-B)Q_n'(z)\\ + 2AnzQ_n(z) + Bz^3Q_n''(z) = -(2n+1-nAz+n^2Bz)Q_n(z) \quad (3.6)\end{aligned}$$

and that

$$\begin{aligned}zP_n'(z) - z^2(A-2Bn+B)P_n'(z) - Bz^3P_n''(z) + (2n+1)Q_n(z) + 2DnzQ_n(z)\\ - 2Dz^2Q_n'(z) - 2zQ_n'(z) = (2n+1-nAz+n^2Bz)P_n(z). \quad (3.7)\end{aligned}$$

Clearly, if we manage to establish (3.6) and (3.7), then (3.5), and hence also (3.1) and (2.2) follow immediately.

Let us write

$$\begin{aligned}p_{n,k} &= p^+_{n,k}\Pi_+ - p^-_{n,k}\Pi_-,\\ q_{n,k} &= q^+_{n,k}\Pi_+ - q^-_{n,k}\Pi_-,\end{aligned}$$

where Π_+ and Π_- are given by (3.2) as before, which implicitly defines the $p^+_{n,k}$'s, etc., and let

$$\begin{aligned}P_n^+(z) &= \sum_{k=0}^n p^+_{n,k}z^k, & P_n^-(z) &= \sum_{k=0}^n p^-_{n,k}z^k,\\ Q_n^+(z) &= \sum_{k=0}^n q^+_{n,k}z^k, & Q_n^-(z) &= \sum_{k=0}^n q^-_{n,k}z^k.\end{aligned}$$

One might hope that (3.6) and (3.7) continue to hold if one replaces $P_n(z)$ by $P_n^+(z)$ and $Q_n(z)$ by $Q_n^+(z)$ everywhere, and that they continue to hold if one replaces $P_n(z)$ by $P_n^-(z)$ and $Q_n(z)$ by $Q_n^-(z)$ everywhere. This turns out to be too optimistic, but not too far from the truth. Our new claim is that

$$\begin{aligned}2CnzP_n^+(z) - 2Cz^2(P_n^+)'(z) - (2n+1)Q_n^+(z) + z(Q_n^+)'(z) - z^2(A+2Bn-B)(Q_n^+)'(z)\\ + 2AnzQ_n^+(z) + Bz^3(Q_n^+)''(z) = -(2n+1-nAz+n^2Bz)Q_n^+(z), \quad (3.8)\end{aligned}$$

$$\begin{aligned}2CnzP_n^-(z) - 2Cz^2(P_n^-)'(z) - (2n+1)Q_n^-(z) + z(Q_n^-)'(z) - z^2(A+2Bn-B)(Q_n^-)'(z)\\ + 2AnzQ_n^-(z) + Bz^3(Q_n^-)''(z) = -(2n+1-nAz+n^2Bz)Q_n^-(z), \quad (3.9)\end{aligned}$$

$$
\begin{aligned}
z(P_n^+)'(z) - z^2(A-2Bn+B)(P_n^+)'(z) - Bz^3(P_n^+)''(z) + (2n+1)Q_n^+(z) + 2DnzQ_n^+(z)\\
- 2Dz^2(Q_n^+)'(z) - 2z(Q_n^+)'(z) = (2n+1-nAz+n^2Bz)P_n^+(z)\\
+ (2n+1)\binom{2n}{n}\frac{(-1)^n B^{-n}\left(\frac{A+2C-E}{2B}\right)_{n+1}}{C\left(\frac{E}{B}-n\right)_{2n+1}},
\end{aligned}
\tag{3.10}
$$

$$
\begin{aligned}
z(P_n^-)'(z) - z^2(A-2Bn+B)(P_n^-)'(z) - Bz^3(P_n^-)''(z) + (2n+1)Q_n^-(z) + 2DnzQ_n^-(z)\\
- 2Dz^2(Q_n^-)'(z) - 2z(Q_n^-)'(z) = (2n+1-nAz+n^2Bz)P_n^-(z)\\
+ (2n+1)\binom{2n}{n}\frac{(-1)^n B^{-n}\left(\frac{A+2C+E}{2B}\right)_{n+1}}{C\left(\frac{E}{B}-n\right)_{2n+1}}.
\end{aligned}
\tag{3.11}
$$

These four equations do indeed imply (3.6) and (3.7): to be precise, by multiplying both sides of (3.8) by Π_+ and multiplying both sides of (3.9) by Π_-, and then taking the difference of the two equations, we obtain (3.6). An analogous argument shows that (3.10) and (3.11) together imply (3.7). Moreover, since

$$
P_n^+(z)\big|_{E\to -E} = -P_n^-(z) \quad \text{and} \quad Q_n^+(z)\big|_{E\to -E} = -Q_n^-(z),
$$

Equation (3.9) results from (3.8) by replacing E by $-E$ (note that the parameter $D=(A^2-E^2)/(4C)$ remains invariant under this replacement), and an analogous assertion holds for (3.10) and (3.11). Thus, the proof of the lemma has been reduced to establishing (3.8) and (3.10).

We start with (3.8). Both sides of this equation are polynomials in z and A (with coefficients depending on n, B, C, E). Due to the form of the coefficients $p_{n,k}^+$ and $q_{n,k}^+$, every subexpression in (3.8) may conveniently (if tediously) be expanded in the basis

$$
\left\{z^k\left(\tfrac{A+2C-E}{2B}\right)_j : j,k=0,1,\dots\right\}.
$$

It can be readily verified that corresponding coefficients on both sides of (3.8) agree.

We use the same approach for (3.10). Again, one readily verifies that corresponding coefficients on both sides of (3.10) agree, except possibly for the coefficients of basis elements of the form $z^0\left(\frac{A+2C-E}{2B}\right)_j$, $j=0,1,\dots$ In other words, we have shown that (3.10) holds except possibly for an error in the coefficient of z^0. There are only three terms in (3.10) which have non-zero coefficient of z^0: the term $(2n+1)Q_n^+(z)$ on the left-hand side, the term $(2n+1)P_n^+(z)$ on the right-hand side, and the last term on the right-hand side. So, in order to completely establish (3.10), we have to show that

$$
(2n+1)q_{n,0}^+ - (2n+1)p_{n,0}^+ = (2n+1)\binom{2n}{n}\frac{(-1)^n B^{-n}\left(\frac{A+2C-E}{2B}\right)_{n+1}}{C\left(\frac{E}{B}-n\right)_{2n+1}},
$$

or, explicitly, that

$$
\begin{aligned}
(2n+1)\frac{(-1)^n B^{-n-1}}{2C\left(\frac{E}{B}-n\right)_{2n+1}}\sum_{j=0}^{n}\binom{n+j}{n}\left(-\tfrac{E}{B}+j+1\right)_{n-j}\left(\tfrac{A+2C-E}{2B}\right)_j\\
\cdot\left(2C+A+\tfrac{2nj}{n+j}B-\tfrac{n-j}{n+j}E\right) = (2n+1)\binom{2n}{n}\frac{(-1)^n B^{-n}\left(\frac{A+2C-E}{2B}\right)_{n+1}}{C\left(\frac{E}{B}-n\right)_{2n+1}}.
\end{aligned}
\tag{3.12}
$$

The Gosper algorithm (cf. [7], [8, § 5.7], [24, § II.5]) finds that

$$(2n+1)\frac{(-1)^n B^{-n-1}}{2C\left(\frac{E}{B}-n\right)_{2n+1}}\binom{n+j}{n}\left(-\tfrac{E}{B}+j+1\right)_{n-j}\left(\tfrac{A+2C-E}{2B}\right)_j \\ \cdot\left(2C+A+\tfrac{2nj}{n+j}B-\tfrac{n-j}{n+j}E\right)=G(n,j+1)-G(n,j), \tag{3.13}$$

with

$$G(n,j)=(2n+1)\frac{(-1)^n B^{-n}}{C\left(\frac{E}{B}-n\right)_{2n+1}}\binom{n+j-1}{n}\left(-\tfrac{E}{B}+j\right)_{n-j+1}\left(\tfrac{A+2C-E}{2B}\right)_j.$$

Clearly, summing both sides of (3.13) over j running from 0 to n immediately yields (3.12), and thus (3.10).

This completes the proof of the lemma. □

Lemma 4. *The differential equation* (2.2) *has a unique solution $R_n(z)=P_n(z)/Q_n(z)$, where $P_n(z)$ and $Q_n(z)$ are polynomials in z of degree at most n, and $P_n(0)=Q_n(0)=1$.*

Proof. The first observation is that the differential equation (2.1) has a unique formal power series solution $F(z)$. This is seen by comparing coefficients of z^m, $m=0,1,\dots$, which allows one to compute the coefficients of the series $F(z)$ recursively. More precisely, comparison of constant coefficients yields that $F(0)=1$, that is, that the coefficient of z^0 in $F(z)$ equals 1, while, for $m\ge 1$, comparison of coefficients of z^m yields an equation which expresses the coefficient of z^m in $F(z)$ uniquely in terms of lower (already computed) coefficients.

Next one observes that the differential equations (2.1) and (2.2) agree for the coefficients of z^m, $m=0,1,\dots,2n$. Thus, what we are computing in (2.2) is the *Padé approximant* of the uniquely determined solution $F(z)$ of (2.1) with the degrees of the numerator and denominator polynomials bounded above by n. Since Padé approximants are unique (see e.g. [2]), a rational function $R_n(z)$ solving (2.2), if there is one at all, is uniquely determined. However, from Lemma 3, we know that such a solution does indeed exist; and, by the arguments above, it is the unique solution of (2.2). □

Remark 5. It should be observed that the above proof of Lemma 4 did not use the precise form of the right-hand side of (2.2). Rather it shows that, if there is a rational function solution of (2.2) of the prescribed form, then this right-hand side is *forced* upon us.

Lemma 6. *The coefficients $p_{n,k}$ and $q_{n,k}$, as defined in* (2.3) *and* (2.4)*, are homogeneous polynomials in A,B,C,D of degree k. In particular, $p_{n,0}=q_{n,0}=1$.*

Proof. We first consider $q_{n,k}$. We shall prove that the expression in (2.4) is a polynomial in A,B,C,E. Taking into account that the denominator can be rewritten as

$$\left(\tfrac{E}{B}-k\right)_{2k+1}=E\prod_{i=1}^{k}\left(\tfrac{E^2}{B^2}-i^2\right), \tag{3.14}$$

and that the term between parentheses in (2.4) is of the form $\operatorname{Pol}(E)-\operatorname{Pol}(-E)$, where $\operatorname{Pol}(E)$ is some polynomial in E, we see that $q_{n,k}$ is a rational function in E^2. Hence, if we are able to show that $q_{n,k}$ is a *polynomial* in A,B,C,E, then, in view of the relation $E^2=A^2-4CD$, it will be obvious that $q_{n,k}$ is also a polynomial in A,B,C,D.

In order to accomplish this, we shall show that the expression between parentheses in (2.4) vanishes for $E = Bs$ with $s = -k, -k+1, \dots, k$. This proves that this expression is divisible by the denominator on the right-hand side of (2.4) (rewritten here in (3.14)) and, after multiplying numerator and denominator of the expression in (2.4) by B^{2k+1}, that $q_{n,k}$ is a homogeneous polynomial in A, B, C, E of degree k, as desired.

Writing the first term between parentheses, with $E = Bs$, in standard hypergeometric notation,

$$
{}_pF_q\left[\begin{matrix}a_1, \dots, a_p \\ b_1, \dots, b_q\end{matrix}; z\right] = \sum_{m=0}^{\infty} \frac{(a_1)_m \cdots (a_p)_m}{m!\,(b_1)_m \cdots (b_q)_m} z^m ,
$$

we get

$$
\begin{aligned}
\left(\tfrac{A+2C+Bs}{2B}\right)_{n+1} &\sum_{j=0}^{k} \binom{k+j}{k}\binom{n-j}{k-j} (-s+j+1)_{k-j} \left(\tfrac{A+2C-Bs}{2B}\right)_j \\
&= \left(\tfrac{A+2C+Bs}{2B}\right)_{n+1} \left(\tfrac{A+2C-Bs}{2B}\right)_s \binom{k+s}{k} \frac{(n-s)!}{(n-k)!} \\
&\qquad \times {}_3F_2\left[\begin{matrix}-k+s, k+s+1, \frac{A}{2B}+\frac{C}{B}+\frac{s}{2} \\ -n+s, s+1\end{matrix}; 1\right]. \qquad (3.15)
\end{aligned}
$$

On the other hand, if we write the second term between parentheses with $E = Bs$ in hypergeometric notation, then we get

$$
\begin{aligned}
\left(\tfrac{A+2C-Bs}{2B}\right)_{n+1} &\sum_{j=0}^{k} \binom{k+j}{k}\binom{n-j}{k-j} (s+j+1)_{k-j} \left(\tfrac{A+2C+Bs}{2B}\right)_j \\
&= \left(\tfrac{A+2C-Bs}{2B}\right)_{n+1} \binom{n}{k} \frac{(k+s)!}{s!}\, {}_3F_2\left[\begin{matrix}-k, k+1, \frac{A}{2B}+\frac{C}{B}+\frac{s}{2} \\ -n, s+1\end{matrix}; 1\right]. \qquad (3.16)
\end{aligned}
$$

In order to see that one expression can be transformed into the other, we apply the transformation formula (see [1, Ex. 7, p. 98])

$$
{}_3F_2\left[\begin{matrix}a, b, c \\ d, e\end{matrix}; 1\right] = \frac{\Gamma(e)\,\Gamma(d+e-a-b-c)}{\Gamma(e-a)\,\Gamma(d+e-b-c)} {}_3F_2\left[\begin{matrix}a, d-b, d-c \\ d, d+e-b-c\end{matrix}; 1\right] \qquad (3.17)
$$

with $a = \frac{A}{2B} + \frac{C}{B} + \frac{s}{2}$, $b = -k$, $c = k+1$, $d = s+1$, $e \to -n$ to (3.16) (here, $\Gamma(x)$ denotes the classical gamma function). After some manipulation, one sees that the result is exactly (3.15).

The arguments for $p_{n,k}$ are completely analogous, albeit more involved due to existence of the extra linear terms in A, C, E in the sums. One additional detail here is that one also has to show that C divides the expression between parentheses in (2.3). In order to see this, one sets $C = 0$ in this expression. In view of $E^2 = A^2 - 4CD$, this specialisation implies that $E = \pm A$. Without loss of generality, we let $E = A$. Then $\left(\frac{A+2C-E}{2B}\right)_j = 0$ for all $j > 0$. Hence, the only term possibly surviving is the one for $j = 0$ in the first sum between parentheses in (2.3). However, for $j = 0$, $C = 0$, and $E = A$ we have $A + \frac{2kj}{k+j}B - \frac{k-j}{k+j}E = A - \frac{k}{k}A = 0$, so that this term vanishes also.

Now, that we already know that $p_{n,0}$ and $q_{n,0}$ are constants, that is, that they are independent of A, B, C, D (or, equivalently, of A, B, C, E), in order to see that in fact $p_{n,0} = q_{n,0} = 1$, we are free to arbitrarily specialise the variables A, B, C, E. Our choice is $A=-2C-n-1$, $B=1$, and $E=-n-1$. Then we have $\left(\frac{A+2C-E}{2B}\right)_{n+1}=(0)_{n+1}=0$, and therefore, in both (2.3) and (2.4), the second term between parentheses vanishes. For the same reason, in the remaining sums over j only the terms for $j=0$ survive, so that we obtain

$$p_{n,0}=\frac{(-1)^{n+1}}{2C\,(-2n-1)_{2n+1}}\,(-n-1)_{n+1}\,(n+2)_n\,(-2C)=1$$

and, similarly,

$$q_{n,0}=\frac{(-1)^{n}}{(-2n-1)_{2n+1}}\,(-n-1)_{n+1}\,(n+2)_n=1.$$

This completes the proof of the lemma. □

Lemma 7. *The coefficients $p_{n,k}$ and $q_{n,k}$, as defined in* (2.3) *and* (2.4), *are polynomials in A,B,C,D with integer coefficients.*

Proof. By Lemma 6, we already know that $p_{n,k}$ and $q_{n,k}$ are polynomials in A,B,C,D. The assertion to be shown here is the *integrality* of the coefficients of these polynomials. In view of Part (4) of Remark 2, since we also know by Lemma 6 that $p_{n,k}$ and $q_{n,k}$ are *homogeneous* polynomials in A,B,C,D, we may without loss of generality set $B=1$, which we shall do for the rest of the argument.

By inspecting the expressions in (2.3) and (2.4), one sees that the only possible obstacle to integrality of coefficients might be powers of 2 appearing in denominators.

The claim is that no denominators occur after one has replaced E^2 by A^2-4CD. The reader should keep in mind that both expressions between parentheses in (2.3) and (2.4) are of the form $\operatorname{Pol}(E)-\operatorname{Pol}(-E)$, where $\operatorname{Pol}(E)$ is some polynomial in E with coefficients depending on n,k,A,C. (We have again suppressed the dependence on variables other than E for the sake of better readability. The reader should recall that $B=1$.) Moreover, the polynomial $\operatorname{Pol}(E)$ may be expanded as a homogeneous polynomial in E and $(A+2C+E)/2$ with integer coefficients. Indeed, that the coefficients are integers is obvious for $q_{n,k}$. For $p_{n,k}$ this is also the case since

$$\binom{k+j}{k}\binom{n-j}{k-j}\frac{2kj}{k+j}=2j\binom{k+j-1}{k-1}\binom{n-j}{k-j}$$

and

$$\binom{k+j}{k}\binom{n-j}{k-j}\frac{k-j}{k+j}=\binom{k+j}{k}\binom{n-j}{k-j}-2\binom{k+j-1}{k}\binom{n-j}{k-j}.$$

So, what we should examine are differences of the form

$$E^a\left(\frac{A+2C+E}{2}\right)^b-(-E)^a\left(\frac{A+2C-E}{2}\right)^b\\
=E^a\left(\left(\frac{A+2C+E}{2}\right)^b\pm\left(\frac{A+2C-E}{2}\right)^b\right). \quad (3.18)$$

We claim that, after the substitution $E^2\to A^2-4CD$, expressions of this form have integer coefficients. Due to the sign $\pm$ in the previous expression, we would have to discuss two different cases. We content ourselves with treating the case where the sign is positive, the other case being completely analogous. Using the multinomial theorem, we expand

$$\left(\frac{A+2C+E}{2}\right)^b+\left(\frac{A+2C-E}{2}\right)^b=2^{1-b}\sum_{\ell_1+\ell_2+2\ell_3=b}\frac{2^{\ell_2}\,b!}{\ell_1!\,\ell_2!\,(2\ell_3)!}A^{\ell_1}C^{\ell_2}E^{2\ell_3},$$

and then substitute A^2-4CD for E^2. Expanding again using the binomial theorem, this leads to the multiple sum

$$2^{1-b}\sum_{\ell_1+\ell_2+2\ell_3=b}\frac{2^{\ell_2}\,b!}{\ell_1!\,\ell_2!\,(2\ell_3)!}A^{\ell_1}C^{\ell_2}\sum_{\ell_4=0}^{\ell_3}(-1)^{\ell_3-\ell_4}\binom{\ell_3}{\ell_4}4^{\ell_3-\ell_4}A^{2\ell_4}C^{\ell_3-\ell_4}D^{\ell_3-\ell_4}.$$

We let $a=\ell_1+2\ell_4$, $d=\ell_3-\ell_4$. With this re-indexing, the above sum is converted into

$$2^{1-b}\sum_{\substack{a,d\ge0\\a+d\le b}}\sum_{\ell_4\ge0}\frac{(-1)^d\,2^{b-a}\,b!\,(d+\ell_4)!}{(a-2\ell_4)!\,(b-a-2d)!\,(2d+2\ell_4)!\,\ell_4!\,d!}A^aC^{b-a-d}D^d.$$

The sum over ℓ_4 can be written in hypergeometric notation, which leads to the expression

$$2^{1-b}\sum_{\substack{a,d\ge0\\a+d\le b}}A^aC^{b-a-d}D^d\frac{(-1)^d\,2^{b-a}\,b!}{a!\,(b-a-2d)!\,(2d)!}{}_2F_1\left[\begin{matrix}-\frac{a}{2},-\frac{a}{2}+\frac{1}{2}\\d+\frac{1}{2}\end{matrix};1\right].$$

This ${}_2F_1$-series can be summed by means of Gauß' summation formula (see [25, (1.7.6); Appendix (III.3)])

$${}_2F_1\left[\begin{matrix}a,b\\c\end{matrix};1\right]=\frac{\Gamma(c)\,\Gamma(c-a-b)}{\Gamma(c-a)\,\Gamma(c-b)}.$$

After some simplification, one arrives at

$$\sum_{\substack{a,d\ge0\\a+d\le b}}(-1)^dA^aC^{b-a-d}D^d\,\frac{a+2d}{a+d}\binom{a+d}{a}\binom{b}{b-a-2d}$$
$$=\sum_{\substack{a,d\ge0\\a+d\le b}}(-1)^dA^aC^{b-a-d}D^d\left(\binom{a+d}{a}+\binom{a+d-1}{a}\right)\binom{b}{b-a-2d}.$$

The integrality of coefficients in expressions of the form (3.18) is now obvious. As we argued above, this implies integrality of coefficients in $q_{n,k}$, and, since — in comparison to $q_{n,k}$ — the expression (2.3) for $p_{n,k}$ contains an additional 2 in the denominator, it implies that all coefficients of $p_{n,k}$ are integers or half-integers (i.e., odd integers divided by 2). To see that the latter coefficients can in fact not be half-integers, let us suppose for a contradiction that $p_{n,k}$ does contain half-integer coefficients, where k is minimal. Because of Lemma 6, which says in particular that $p_{n,0}=q_{n,0}=1$, we must have $k>0$. We then consider the coefficient of z^k on the left-hand side of (3.1). It contains the term $p_{n,k}q_{n,0}=p_{n,k}$, and otherwise only terms involving $p_{n,j}$'s with $j<k$ and $q_{n,j}$'s with $j\le k$. Since the coefficient of z^k on the right-hand side equals zero, this means that $p_{n,k}$ is given in terms of expressions which we know by our minimality assumption to be polynomials in A,B,C,D with integer coefficients. The coefficient $p_{n,k}$ must therefore

have the same property, contradicting our assumption that $p_{n,k}$ contains half-integer coefficients. This completes the proof of the lemma. $\square$

4. Free subgroup numbers for lifts of $\mathrm{PSL}_2(\mathbb{Z})$ modulo prime powers

For integers m, $\lambda \geq 1$, let $f_\lambda(m)$ denote the number of free subgroups of index $6m\lambda$ in the lift $\Gamma_m(3)$ of $\mathrm{PSL}_2(\mathbb{Z})$ defined by (1.1); in particular, $f_\lambda := f_\lambda(1)$ is the number of free subgroups in the inhomogeneous modular group $\mathrm{PSL}_2(\mathbb{Z})$ of index 6λ. Our original motivation, when embarking on this project, was to establish the following result, which now is an easy consequence of Theorem 1.

Theorem 8. *Let m be a positive integer, p a prime number with $p \geq 5$, and let α be a positive integer. Then the generating function $F_m(z) = 1 + \sum_{\lambda\geq 1} f_\lambda(m)z^\lambda$, when coefficients are reduced modulo p^α, can be represented as a rational function. Equivalently, the sequence $(f_\lambda(m))_{\lambda\geq 1}$ is ultimately periodic modulo p^α.*

Proof. It is well-known that $F_m(z)$ satisfies the differential equation[2]

$$(1-(6m-2)z)F_m(z) - 6mz^2F_m'(z) - zF_m^2(z) - 1 - (1-6m+5m^2)z = 0. \tag{4.1}$$

By specialising $A = 6m-2$, $B = 6m$, $C = 1$, and $D = 1-6m+5m^2$ in Theorem 1, we infer that there exist polynomials $P_n^{(m)}(z)$ and $Q_n^{(m)}(z)$ such that $R_n^{(m)}(z) = P_n^{(m)}(z)/Q_n^{(m)}(z)$ satisfies

$$\begin{multline}(1-(6m-2)z)R_n^{(m)}(z) - 6mz^2\left(R_n^{(m)}\right)'(z) - z\left(R_n^{(m)}\right)^2(z) - 1 - (1-6m+5m^2)z\\ = -\frac{5m^{2n+2}z^{2n+1}}{\left(Q_n^{(m)}\right)^2(z)}\prod_{\ell=1}^{n}(6\ell+1)(6\ell+5). \tag{4.2}\end{multline}$$

If we now choose n large enough then, since p^α is coprime to 6, the right-hand side will vanish modulo p^α. Since the differential equation (4.1) determines a unique formal power series solution, even when coefficients are reduced modulo a prime p (this is seen in the same way as in the beginning of the proof of Lemma 4), this proves our claim. $\square$

5. Some more precise results

Recall that the generating function $F_m(z) = 1 + \sum_{\lambda\geq 1} f_\lambda(m)\, z^\lambda$ for the numbers of free subgroups in $\Gamma_m(3)$ satisfies the Riccati differential equation (4.1), which is the special case of (2.1) in which $A = 6m-2$, $B = 6m$, $C = 1$, and $D = 1-6m+5m^2$.

The following two lemmas are the key for deriving the main result of this section, Theorem 11, which identifies the denominators of the rational functions which one obtains when the coefficients of the generating function $1 + \sum_{\lambda\geq 1} f_\lambda(m)z^\lambda$ are reduced modulo a prime power p^α with $p \geq 5$. In the statement of the lemmas, and also later, we write

$$f(z) = g(z) \text{ modulo } m$$

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

[2]Cf. [12, Formula (8.1)] for this, or Formula (18) in [18, Sec. 2.3] with $F_m(z) = 1 + z\beta_{\Gamma_m(3)}(z)$ for the same result in a more general context.

Lemma 9. *Let p be a prime with $p \equiv 1 \pmod 6$. For $A = 6m-2$, $B = 6m$, $C = 1$, $D = 1-6m+5m^2$ (and, hence, $E = 4m$), and $n \equiv \frac{p-1}{6}, \frac{5(p-1)}{6} \pmod p$, we have*

$$Q_n(z) = Q_{(p-1)/6}(z) \quad \text{modulo } p,$$

with $Q_n(z)$ as given in the assertion of Theorem 1. Furthermore, if $p \nmid m$, then the polynomial $Q_{(p-1)/6}(z)$ has degree $(p-1)/6$ in z when coefficients are reduced modulo p, whereas $Q_{(p-1)/6}(z) = 1$ modulo p if $p \mid m$.

Proof. We specialise the result of Theorem 1 to $A = 6m-2$, $B = 6m$, $C = 1$, $D = 1-6m+5m^2$, to see that $R_n(z) = P_n(z)/Q_n(z)$ solves (4.1), where $Q_n(z) = \sum_{k=0}^{n} q_{n,k} z^k$, with coefficients given by

$$q_{n,n-k} = \frac{(-1)^n 6^{n-k} m^{n-k}}{(\frac{2}{3}-k)_{2k+1}} \Bigg(\left(\tfrac{5}{6}\right)_{n+1} \sum_{j=0}^{k} \binom{k+j}{k} \binom{n-j}{k-j} \left(-\tfrac{2}{3}+j+1\right)_{k-j} \left(\tfrac{1}{6}\right)_j \\ - \left(\tfrac{1}{6}\right)_{n+1} \sum_{j=0}^{k} \binom{k+j}{k} \binom{n-j}{k-j} \left(\tfrac{2}{3}+j+1\right)_{k-j} \left(\tfrac{5}{6}\right)_j \Bigg). \tag{5.1}$$

The reader should observe that the only dependence on m of $q_{n,n-k}$ is in the term m^{n-k} which occurs right in the front of the above expression. Hence, since by Theorem 1 we know that $q_{n,0} = 1$, we have $Q_{(p-1)/6}(z) = 1$ modulo p if $p \mid m$. On the other hand, if $p \nmid m$, from (3.4) it is easy to see that $q_{(p-1)/6,(p-1)/6} \not\equiv 0 \pmod p$ for $A = 6m-2$, $B = 6m$, $C = 1$, $D = 1-6m+5m^2$, $E = 4m$. (As a matter of fact, with this choice of parameters, we have $\Pi_+ \not\equiv 0 \pmod p$, whereas $\Pi_- \equiv 0 \pmod p$.) So, indeed, if $p \nmid m$ the polynomial $Q_{(p-1)/6}(z)$ has degree $(p-1)/6$ in z when coefficients are reduced modulo p.

What remains to show is that all coefficients $q_{n,n-k}$, $0 \le k \le n - \frac{p-1}{6} - 1$, are divisible by p for the specialisation of the parameters A, B, C, D, E considered here.

In order to see this, we start by writing the sums over j in (5.1) in hypergeometric notation, thus obtaining

$$q_{n,n-k} = \frac{(-1)^n 6^{n-k} m^{n-k}}{(\frac{2}{3}-k)_{2k+1}} \Bigg(\left(\tfrac{5}{6}\right)_{n+1} \binom{n}{k} \left(\tfrac{1}{3}\right)_k {}_3F_2\left[\begin{matrix} \frac{1}{6}, k+1, -k \\ \frac{1}{3}, -n \end{matrix}; 1\right] \\ - \left(\tfrac{1}{6}\right)_{n+1} \binom{n}{k} \left(\tfrac{5}{3}\right)_k {}_3F_2\left[\begin{matrix} \frac{5}{6}, k+1, -k \\ \frac{5}{3}, -n \end{matrix}; 1\right] \Bigg).$$

Next we apply the transformation formula (3.17) one more time, here with $a = -k$. This converts the last expression into

$$q_{n,n-k} = \frac{(-1)^n 6^{n-k} m^{n-k}}{(\frac{2}{3}-k)_{2k+1}} \Bigg(\left(\tfrac{5}{6}\right)_{n+1} \frac{(-1)^k}{k!} \left(\tfrac{1}{3}\right)_k \left(-n-k-\tfrac{5}{6}\right)_k \, {}_3F_2\left[\begin{matrix} \frac{1}{6}, -k-\frac{2}{3}, -k \\ \frac{1}{3}, -n-k-\frac{5}{6} \end{matrix}; 1\right] \\ - \left(\tfrac{1}{6}\right)_{n+1} \frac{(-1)^k}{k!} \left(\tfrac{5}{3}\right)_k \left(-n-k-\tfrac{1}{6}\right)_k \, {}_3F_2\left[\begin{matrix} \frac{5}{6}, -k+\frac{2}{3}, -k \\ \frac{5}{3}, -n-k-\frac{1}{6} \end{matrix}; 1\right] \Bigg) \\ = (-1)^n 6^{n-k} m^{n-k} \Bigg(\sum_{j=0}^{k} \frac{(-1)^{k+j}}{k!} \binom{k}{j} \frac{\left(\frac{5}{6}-j\right)_{n+k+1}}{\left(\frac{2}{3}-j\right)_{k+1}} \\ + \sum_{j=0}^{k} \frac{(-1)^{k+j}}{k!} \binom{k}{j} \frac{\left(\frac{1}{6}-j\right)_{n+k+1}}{\left(-\frac{2}{3}-j\right)_{k+1}} \Bigg). \tag{5.2}$$

We claim that, if $n \equiv \frac{p-1}{6}, \frac{5(p-1)}{6} \pmod p$ and $n \ge k + \frac{p-1}{6} + 1$, then each summand in the sums over j is divisible by p.

To see this, we first consider the expression

$$\frac{(-1)^{k+j}}{k!} \binom{k}{j} \frac{\left(\frac{5}{6}-j\right)_{n+k+1}}{\left(\frac{2}{3}-j\right)_{k+1}}.$$

Let $v_p(\alpha)$ denote the p-adic valuation of the integer α, that is, the maximal exponent e such that p^e divides α. By variations of the well-known formula of Legendre [17, p. 10] for the p-adic valuation of factorials, we have

$$v_p\left(\frac{(-1)^{k+j}}{k!} \binom{k}{j} \frac{\left(\frac{5}{6}-j\right)_{n+k+1}}{\left(\frac{2}{3}-j\right)_{k+1}} \right) = \sum_{\ell=1}^{\infty} \Bigg(-\left\lfloor \frac{j}{p^\ell} \right\rfloor - \left\lfloor \frac{k-j}{p^\ell} \right\rfloor + \left\lfloor \frac{n+k-j+\frac{1}{6}(p^\ell+5)}{p^\ell} \right\rfloor \\ - \left\lfloor \frac{-j+\frac{1}{6}(p^\ell-1)}{p^\ell} \right\rfloor - \left\lfloor \frac{k-j+\frac{1}{3}(p^\ell+2)}{p^\ell} \right\rfloor + \left\lfloor \frac{-j+\frac{1}{3}(p^\ell-1)}{p^\ell} \right\rfloor \Bigg). \tag{5.3}$$

We need to prove that this sum over ℓ is at least 1. In the case where $\ell = 1$, the summand reduces to

$$-\left\lfloor \frac{j}{p} \right\rfloor - \left\lfloor \frac{k-j}{p} \right\rfloor \\ + \left\lfloor \frac{n+k-j+\frac{5}{6}}{p} + \frac{1}{6} \right\rfloor - \left\lfloor \frac{-j-\frac{1}{6}}{p} + \frac{1}{6} \right\rfloor - \left\lfloor \frac{k-j+\frac{2}{3}}{p} + \frac{1}{3} \right\rfloor + \left\lfloor \frac{-j-\frac{1}{3}}{p} + \frac{1}{3} \right\rfloor.$$

Let us write $N = \{n/p\}$, $K = \{k/p\}$, and $J = \{j/p\}$, where $\{\alpha\} := \alpha - \lfloor \alpha \rfloor$ denotes the fractional part of α. With this notation, the last expression becomes

$$\left\lfloor \frac{n}{p} \right\rfloor - \left\lfloor \frac{k}{p} \right\rfloor - \lfloor K-J \rfloor \\ + \left\lfloor N+K-J+\frac{5}{6p}+\frac{1}{6} \right\rfloor - \left\lfloor -J-\frac{1}{6p}+\frac{1}{6} \right\rfloor - \left\lfloor K-J+\frac{2}{3p}+\frac{1}{3} \right\rfloor + \left\lfloor -J-\frac{1}{3p}+\frac{1}{3} \right\rfloor. \tag{5.4}$$

If $n \equiv \frac{p-1}{6} \pmod p$, then $N = \frac{p-1}{6p}$. Hence,

$$\left\lfloor N + K - J + \frac{5}{6p} + \frac{1}{6} \right\rfloor - \left\lfloor K - J + \frac{2}{3p} + \frac{1}{3} \right\rfloor = 0.$$

Moreover, since $k \le n - \frac{p-1}{6} - 1$, we have $\left\lfloor \frac{n}{p} \right\rfloor - \left\lfloor \frac{k}{p} \right\rfloor \ge 1$. Since, trivially, $-\lfloor K - J \rfloor \ge 0$ and $-\left\lfloor -J - \frac{1}{6p} + \frac{1}{6} \right\rfloor + \left\lfloor -J - \frac{1}{3p} + \frac{1}{3} \right\rfloor \ge 0$, the expression in (5.4) is at least 1.

On the other hand, if $n \equiv \frac{5(p-1)}{6} \pmod p$, then $N = \frac{5(p-1)}{6p}$. In this case, we have

$$-\lfloor K - J \rfloor + \left\lfloor N + K - J + \frac{5}{6p} + \frac{1}{6} \right\rfloor = 1,$$

we have certainly $\left\lfloor \frac{n}{p} \right\rfloor - \left\lfloor \frac{k}{p} \right\rfloor \ge 0$, and, again, $-\left\lfloor -J - \frac{1}{6p} + \frac{1}{6} \right\rfloor + \left\lfloor -J - \frac{1}{3p} + \frac{1}{3} \right\rfloor \ge 0$. If we suppose that $-\left\lfloor K - J + \frac{2}{3p} + \frac{1}{3} \right\rfloor = -1$, then K must be at least $\frac{2}{3p}(p-1)$, or, equivalently, $k \equiv \frac{2}{3}(p-1), \frac{2}{3}(p-1)+1, \dots, p-1 \pmod p$. But, because of $n \ge k + \frac{p-1}{6} + 1$ and $n \equiv \frac{5(p-1)}{6} \pmod p$, this implies $\left\lfloor \frac{n}{p} \right\rfloor - \left\lfloor \frac{k}{p} \right\rfloor \ge 1$. Hence, in all cases the expression in (5.4) is at least 1.

Now we have to discuss the summand in (5.3) when $\ell \ge 2$. Similarly to above, we write $N = \{n/p^\ell\}$, $K = \{k/p^\ell\}$, and $J = \{j/p^\ell\}$. Using this notation, we may rewrite this summand as

$$\begin{aligned} \left\lfloor \frac{n}{p^\ell} \right\rfloor - \left\lfloor \frac{k}{p^\ell} \right\rfloor - \lfloor K - J \rfloor + \left\lfloor N + K - J + \frac{1}{6} + \frac{5}{6 \cdot p^\ell} \right\rfloor - \left\lfloor -J + \frac{1}{6} - \frac{1}{6 \cdot p^\ell} \right\rfloor \\ - \left\lfloor K - J + \frac{1}{3} + \frac{2}{3 \cdot p^\ell} \right\rfloor + \left\lfloor -J + \frac{1}{3} - \frac{1}{3 \cdot p^\ell} \right\rfloor . \end{aligned} \tag{5.5}$$

We have $-\left\lfloor -J + \frac{1}{6} - \frac{1}{6 \cdot p^\ell} \right\rfloor + \left\lfloor -J + \frac{1}{3} - \frac{1}{3 \cdot p^\ell} \right\rfloor \ge 0$, $-\lfloor K - J \rfloor \ge 0$, and, since $n \ge k + \frac{p-1}{6} + 1$, also $\left\lfloor \frac{n}{p^\ell} \right\rfloor - \left\lfloor \frac{k}{p^\ell} \right\rfloor \ge 0$. If

$$\left\lfloor N + K - J + \frac{1}{6} + \frac{5}{6 \cdot p^\ell} \right\rfloor - \left\lfloor K - J + \frac{1}{3} + \frac{2}{3 \cdot p^\ell} \right\rfloor \ge 0, \tag{5.6}$$

then (5.5) is non-negative. There are two cases where (5.6) is violated. It should be noted that then the left-hand side of (5.6) equals -1. Violation of (5.6) can either happen if

$$N + K - J + \frac{1}{6} + \frac{5}{6 \cdot p^\ell} < 0 \le K - J + \frac{1}{3} + \frac{2}{3 \cdot p^\ell},$$

in which case necessarily $K - J < 0$ and thus actually $-\lfloor K - J \rfloor = 1$, or if

$$N + K - J + \frac{1}{6} + \frac{5}{6 \cdot p^\ell} < 1 \le K - J + \frac{1}{3} + \frac{2}{3 \cdot p^\ell}.$$

In the latter case, we have in particular $K \ge \frac{2}{3} - \frac{2}{3 \cdot p^\ell}$, and on the other hand

$$N \le N + K - J - \frac{2}{3} + \frac{2}{3 \cdot p^\ell} < \frac{1}{6} - \frac{1}{6 \cdot p^\ell}.$$

Again, since $n \ge k + \frac{p-1}{6} + 1$, this implies that actually $\left\lfloor \frac{n}{p^\ell} \right\rfloor - \left\lfloor \frac{k}{p^\ell} \right\rfloor \ge 1$, so that in all cases the expression in (5.5) is non-negative.

This proves that the sum on the right-hand side of (5.3) is at least 1, which, in turn, means that all summands in the first sum over j on the right-hand side of (5.2) are divisible by p.

Next, we consider the expression

$$\frac{(-1)^{k+j}}{k!}\binom{k}{j}\frac{\left(\frac{1}{6}-j\right)_{n+k+1}}{\left(-\frac{2}{3}-j\right)_{k+1}}.$$

Here, we see that

$$\begin{aligned} v_p&\left(\frac{(-1)^{k+j}}{k!}\binom{k}{j}\frac{\left(\frac{1}{6}-j\right)_{n+k+1}}{\left(-\frac{2}{3}-j\right)_{k+1}}\right)\\ &=\sum_{\ell=1}^{\infty}\Bigg(-\left\lfloor\frac{j}{p^\ell}\right\rfloor-\left\lfloor\frac{k-j}{p^\ell}\right\rfloor+\left\lfloor\frac{n+k-j+\frac{1}{6}(5\cdot p^\ell+1)}{p^\ell}\right\rfloor\\ &\qquad-\left\lfloor\frac{-j+\frac{5}{6}(p^\ell-1)}{p^\ell}\right\rfloor-\left\lfloor\frac{k-j+\frac{2}{3}(p^\ell-1)}{p^\ell}\right\rfloor+\left\lfloor\frac{-j+\frac{1}{3}(2\cdot p^\ell-5)}{p^\ell}\right\rfloor\Bigg). \end{aligned} \tag{5.7}$$

Again, we have to prove that this sum over ℓ is at least 1. In the case where $\ell = 1$, the summand reduces to

$$\begin{aligned} &-\left\lfloor\frac{j}{p}\right\rfloor-\left\lfloor\frac{k-j}{p}\right\rfloor\\ &\quad+\left\lfloor\frac{n+k-j+\frac{1}{6}}{p}+\frac{5}{6}\right\rfloor-\left\lfloor\frac{-j-\frac{5}{6}}{p}+\frac{5}{6}\right\rfloor-\left\lfloor\frac{k-j-\frac{2}{3}}{p}+\frac{2}{3}\right\rfloor+\left\lfloor\frac{-j-\frac{5}{3}}{p}+\frac{2}{3}\right\rfloor. \end{aligned}$$

With the notation $N = \{n/p\}$, $K = \{k/p\}$, and $J = \{j/p\}$, as before, the last expression becomes

$$\begin{aligned} &\left\lfloor\frac{n}{p}\right\rfloor-\left\lfloor\frac{k}{p}\right\rfloor-\lfloor K-J\rfloor\\ &+\left\lfloor N+K-J+\frac{1}{6p}+\frac{5}{6}\right\rfloor-\left\lfloor -J-\frac{5}{6p}+\frac{5}{6}\right\rfloor-\left\lfloor K-J-\frac{2}{3p}+\frac{2}{3}\right\rfloor+\left\lfloor -J-\frac{5}{3p}+\frac{2}{3}\right\rfloor. \end{aligned} \tag{5.8}$$

If $n \equiv \frac{p-1}{6} \pmod p$, then $N = \frac{p-1}{6p}$. Hence,

$$\left\lfloor N+K-J+\frac{1}{6p}+\frac{5}{6}\right\rfloor-\lfloor K-J\rfloor=1.$$

Moreover, since $k \le n - \frac{p-1}{6} - 1$, we have $\left\lfloor \frac{n}{p} \right\rfloor - \left\lfloor \frac{k}{p} \right\rfloor \ge 1$. If

$$-\left\lfloor -J-\frac{5}{6p}+\frac{5}{6}\right\rfloor+\left\lfloor -J-\frac{5}{3p}+\frac{2}{3}\right\rfloor=-1,$$

then $J = \frac{2(p-1)}{3p}, \frac{2(p-1)}{3p} + 1, \dots, p-1$, and in all cases it follows that

$$-\left\lfloor K - J - \frac{2}{3p} + \frac{2}{3} \right\rfloor \geq 0.$$

Therefore the expression in (5.8) is at least 1.

On the other hand, if $n \equiv \frac{5(p-1)}{6} \pmod p$, then $N = \frac{5(p-1)}{6p}$. In this case, we have

$$\left\lfloor N + K - J + \frac{1}{6p} + \frac{5}{6} \right\rfloor - \left\lfloor K - J - \frac{2}{3p} + \frac{2}{3} \right\rfloor = 1$$

and $\left\lfloor \frac{n}{p} \right\rfloor - \left\lfloor \frac{k}{p} \right\rfloor \geq 0$. Again, if $-\left\lfloor -J - \frac{5}{6p} + \frac{5}{6} \right\rfloor + \left\lfloor -J - \frac{5}{3p} + \frac{2}{3} \right\rfloor = -1$, then $J = \frac{2(p-1)}{3p}, \frac{2(p-1)}{3p} + 1, \dots, p-1$, and in all cases it follows that

$$-\lfloor K - J \rfloor \geq -\left\lfloor K - \frac{2(p-1)}{3p} \right\rfloor \geq 0.$$

If $\lfloor K - J \rfloor = 0$ (that is, if $-\lfloor K - J \rfloor \neq 1$), so that in particular $K \geq \frac{2(p-1)}{3p}$, then, since $n \equiv \frac{5(p-1)}{6} \pmod p$ and $n \geq k + \frac{p-1}{6} + 1$, we actually have $\left\lfloor \frac{n}{p} \right\rfloor - \left\lfloor \frac{k}{p} \right\rfloor \geq 1$. Hence, in all cases the expression in (5.8) is at least 1.

We turn to the summand in (5.7) when $\ell \geq 2$. Writing $N = \{n/p^\ell\}$, $K = \{k/p^\ell\}$, and $J = \{j/p^\ell\}$, this summand acquires the form

$$\begin{aligned} &\left\lfloor \frac{n}{p^\ell} \right\rfloor - \left\lfloor \frac{k}{p^\ell} \right\rfloor - \lfloor K - J \rfloor + \left\lfloor N + K - J + \frac{5}{6} + \frac{1}{6 \cdot p^\ell} \right\rfloor \\ &\quad - \left\lfloor -J + \frac{5}{6} - \frac{5}{6 \cdot p^\ell} \right\rfloor - \left\lfloor K - J + \frac{2}{3} - \frac{2}{3 \cdot p^\ell} \right\rfloor + \left\lfloor -J + \frac{2}{3} - \frac{5}{3 \cdot p^\ell} \right\rfloor. \end{aligned} \tag{5.9}$$

Clearly, we have $-\lfloor K - J \rfloor \geq 0$, we have

$$\left\lfloor N + K - J + \frac{5}{6} + \frac{1}{6 \cdot p^\ell} \right\rfloor - \left\lfloor K - J + \frac{2}{3} - \frac{2}{3 \cdot p^\ell} \right\rfloor \geq 0,$$

and, since $n \geq k + \frac{p-1}{6} + 1$, also $\left\lfloor \frac{n}{p^\ell} \right\rfloor - \left\lfloor \frac{k}{p^\ell} \right\rfloor \geq 0$. If

$$-\left\lfloor -J + \frac{5}{6} - \frac{5}{6 \cdot p^\ell} \right\rfloor + \left\lfloor -J + \frac{2}{3} - \frac{5}{3 \cdot p^\ell} \right\rfloor \geq 0, \tag{5.10}$$

then (5.9) is non-negative. The inequality (5.10) is only violated if $\frac{5}{6} - \frac{5}{6 \cdot p^\ell} \geq J > \frac{2}{3} - \frac{5}{3 \cdot p^\ell}$, in which case the left-hand side of (5.10) equals -1. It follows that $K - J + \frac{2}{3} - \frac{2}{3 \cdot p^\ell} < K + \frac{1}{p^\ell} \leq 1$, so that $\left\lfloor K - J + \frac{2}{3} - \frac{2}{3 \cdot p^\ell} \right\rfloor \leq 0$, that is, equivalently, $-\left\lfloor K - J + \frac{2}{3} - \frac{2}{3 \cdot p^\ell} \right\rfloor \geq 0$. If we now suppose that both $-\lfloor K - J \rfloor$ and $\left\lfloor N + K - J + \frac{5}{6} + \frac{1}{6 \cdot p^\ell} \right\rfloor$ are zero (that is, not 1), then $K \geq J$ and $N + K - J + \frac{5}{6} + \frac{1}{6 \cdot p^\ell} < 1$, and this entails the inequality chain

$$1 > N + K - J + \frac{5}{6} + \frac{1}{6 \cdot p^\ell} \geq N + K + \frac{1}{p^\ell}.$$

On the other hand, since $K \ge J > \frac{2}{3} - \frac{5}{3 \cdot p^\ell}$, the number N can be at most $1/3$. Because of $n \ge k + \frac{p-1}{6} + 1$, this implies that actually $\left\lfloor \frac{n}{p^\ell} \right\rfloor - \left\lfloor \frac{k}{p^\ell} \right\rfloor \ge 1$, so that in all cases the expression in (5.9) is non-negative.

This proves that the sum on the right-hand side of (5.7) is at least 1, which, in its turn, means that all summands in the second sum over j on the right-hand side of (5.2) are divisible by p, completing the proof of the lemma. □

Lemma 10. *Let p be a prime with $p \equiv 5 \pmod 6$. For $A = 6m - 2$, $B = 6m$, $C = 1$, $D = 1 - 6m + 5m^2$ (and, hence, $E = 4m$), and $n \equiv \frac{p-5}{6}, \frac{5p-1}{6} \pmod p$, we have*

$$Q_n(z) = Q_{(p-5)/6}(z) \quad \text{modulo } p,$$

with $Q_n(z)$ as given in Theorem 1. Furthermore, if $p \nmid m$, then the polynomial $Q_{(p-5)/6}(z)$ has degree $(p-5)/6$ in z when coefficients are reduced modulo p, whereas $Q_{(p-5)/6}(z) = 1$ modulo p if $p \mid m$.

Proof. This assertion may be established in a fashion similar to the proof of Lemma 9. The assertion about the degree of $Q_{(p-5)/6}(z)$ is straightforward to see.

In order to prove the congruence, we would again use the form (5.2) for $q_{n,n-k}$. Here, we have

$$\begin{aligned} v_p\left(\frac{(-1)^{k+j}}{k!}\binom{k}{j}\frac{\left(\frac{5}{6}-j\right)_{n+k+1}}{\left(\frac{2}{3}-j\right)_{k+1}}\right) &= \sum_{\substack{\ell=1\\ \ell \text{ even}}}^{\infty}\left(-\left\lfloor\frac{j}{p^\ell}\right\rfloor - \left\lfloor\frac{k-j}{p^\ell}\right\rfloor + \left\lfloor\frac{n+k-j+\frac{1}{6}(p^\ell+5)}{p^\ell}\right\rfloor\right.\\ &\qquad \left. - \left\lfloor\frac{-j+\frac{1}{6}(p^\ell-1)}{p^\ell}\right\rfloor - \left\lfloor\frac{k-j+\frac{1}{3}(p^\ell+2)}{p^\ell}\right\rfloor + \left\lfloor\frac{-j+\frac{1}{3}(p^\ell-1)}{p^\ell}\right\rfloor\right)\\ &+ \sum_{\substack{\ell=1\\ \ell \text{ odd}}}^{\infty}\left(-\left\lfloor\frac{j}{p^\ell}\right\rfloor - \left\lfloor\frac{k-j}{p^\ell}\right\rfloor + \left\lfloor\frac{n+k-j+\frac{5}{6}(p^\ell+1)}{p^\ell}\right\rfloor\right.\\ &\qquad \left. - \left\lfloor\frac{-j+\frac{1}{6}(5p^\ell-1)}{p^\ell}\right\rfloor - \left\lfloor\frac{k-j+\frac{2}{3}(p^\ell+1)}{p^\ell}\right\rfloor + \left\lfloor\frac{-j+\frac{1}{3}(2p^\ell-1)}{p^\ell}\right\rfloor\right) \end{aligned} \tag{5.11}$$

and

$$
\begin{aligned}
&v_p\left(\frac{(-1)^{k+j}}{k!}\binom{k}{j}\frac{\left(\frac{1}{6}-j\right)_{n+k+1}}{\left(-\frac{2}{3}-j\right)_{k+1}}\right)\\
&\qquad=\sum_{\substack{\ell=1\\ \ell\text{ even}}}^{\infty}\left(-\left\lfloor\frac{j}{p^\ell}\right\rfloor-\left\lfloor\frac{k-j}{p^\ell}\right\rfloor+\left\lfloor\frac{n+k-j+\frac{1}{6}(5p^\ell+1)}{p^\ell}\right\rfloor\right.\\
&\qquad\qquad\left.-\left\lfloor\frac{-j+\frac{5}{6}(p^\ell-1)}{p^\ell}\right\rfloor-\left\lfloor\frac{k-j+\frac{2}{3}(p^\ell-1)}{p^\ell}\right\rfloor+\left\lfloor\frac{-j+\frac{1}{3}(2p^\ell-5)}{p^\ell}\right\rfloor\right)\\
&\quad+\sum_{\substack{\ell=1\\ \ell\text{ odd}}}^{\infty}\left(-\left\lfloor\frac{j}{p^\ell}\right\rfloor-\left\lfloor\frac{k-j}{p^\ell}\right\rfloor+\left\lfloor\frac{n+k-j+\frac{1}{6}(p^\ell+1)}{p^\ell}\right\rfloor\right.\\
&\qquad\qquad\left.-\left\lfloor\frac{-j+\frac{1}{6}(p^\ell-5)}{p^\ell}\right\rfloor-\left\lfloor\frac{k-j+\frac{1}{3}(2p^\ell-1)}{p^\ell}\right\rfloor+\left\lfloor\frac{-j+\frac{1}{3}(2p^\ell-4)}{p^\ell}\right\rfloor\right),
\end{aligned}
\tag{5.12}
$$

and these are the expressions which have to be analysed p-adically. We leave it to the interested reader to fill in the details. □

Theorem 11. *Let α be a positive integer. If p is a prime with $p \equiv 1 \pmod 6$, then the generating function $F_m(z) = 1 + \sum_{\lambda\ge1} f_\lambda(m)\, z^\lambda$, when coefficients are reduced modulo p^α, equals $\overline{P}_\alpha(z)/Q^\alpha_{(p-1)/6}(z)$, where $\overline{P}_\alpha(z)$ is a polynomial in z over the integers, and $Q_{(p-1)/6}(z)$ is the polynomial of degree $(p-1)/6$ given by the formula in Theorem 1 with $A = 6m-2$, $B = 6m$, $C = 1$, $D = 1-6m+5m^2$ and $E = 4m$.*

On the other hand, if p is a prime with $p \equiv 5 \pmod 6$, then the generating function $F_m(z) = 1 + \sum_{\lambda\ge1} f_\lambda(m)\, z^\lambda$, when coefficients are reduced modulo p^α, equals $\widehat{P}_\alpha(z)/Q^\alpha_{(p-5)/6}(z)$, where $\widehat{P}_\alpha(z)$ is a polynomial in z over the integers, and $Q_{(p-5)/6}(z)$ is the polynomial of degree $(p-5)/6$ given by the formula in Theorem 1 with $A = 6m-2$, $B = 6m$, $C = 1$, $D = 1-6m+5m^2$ and $E = 4m$.

Proof. We proceed by induction on α.

For the start of the induction, we just have to use Theorem 1 with $A = 6m-2$, $B = 6m$, $C = 1$, $D = 1-6m+5m^2$, $E = 4m$, and choose $n = (p-1)/6$ and $n = (p-5)/6$, respectively, as this makes the product on the right-hand side of (2.2) vanish. By uniqueness of the solution of (4.1), it follows that

$$F_m(z) = \frac{P_d(z)}{Q_d(z)} \quad \text{modulo } p,$$

where $d = (p-1)/6$ or $d = (p-5)/6$, depending on the congruence class of p modulo 6.

Let us now suppose that we have already found an integer polynomial $A_\alpha(z)$ such that $F_\alpha(z) := A_\alpha(z)/Q^\alpha_d(z)$ solves (4.1) modulo p^α for some $\alpha \ge 1$. We choose $n \equiv \frac{p-1}{6} \pmod p$ or $n \equiv \frac{p-5}{6} \pmod p$, respectively, large enough such that the product over ℓ on the right-hand side of (4.2) vanishes modulo $p^{\alpha+1}$. (The reader should recall that the specialisation $A = 6m-2$, $B = 6m$, $C = 1$, $D = 1-6m+5m^2$, $E = 4m$, which is considered here, corresponds to the specialisation of Theorem 1 considered in

Theorem 8). By uniqueness of solution of the differential equation (4.2) (see Theorem 1), we must then have

$$R_n(z) = F_\alpha(z) \quad \text{modulo } p^\alpha, \tag{5.13}$$

where $R_n(z) = R_n^{(1)}(z) = P_n(z)/Q_n(z)$ is the solution to (4.2) given by Theorem 1. Consequently, if we consider the difference,

$$R_n(z) - F_\alpha(z) = \frac{P_n(z)}{Q_n(z)} - \frac{A_\alpha(z)}{Q_d^\alpha(z)} = \frac{P_n(z)Q_d^\alpha(z) - A_\alpha(z)Q_n(z)}{Q_d^\alpha(z)Q_n(z)},$$

then, since $Q_d^\alpha(z)Q_n(z)$ has constant coefficient 1 (see Theorem 1), we know by (5.13) that all coefficients of the integer polynomial in the numerator of the last fraction must be divisible by p^α. In other words, there is an integer polynomial $B_\alpha(z)$ such that

$$R_n(z) = F_\alpha(z) + p^\alpha \frac{B_\alpha(z)}{Q_d^\alpha(z)Q_n(z)}.$$

If we consider both sides of this equation modulo $p^{\alpha+1}$, then the fraction which is multiplied by p^α may be reduced modulo p. By Lemmas 9 and 10, this leads to the congruence

$$R_n(z) = \frac{A_\alpha(z)}{Q_d^\alpha(z)} + p^\alpha \frac{B_\alpha(z)}{Q_d^{\alpha+1}(z)} \quad \text{modulo } p^{\alpha+1}. \tag{5.14}$$

So, indeed, the solution $R_n(z)$ to the Riccati differential equation (4.1), when coefficients of series are reduced modulo $p^{\alpha+1}$, can be expressed as a rational function with denominator $Q_d^{\alpha+1}(z)$, where $d = (p-1)/6$ in case $p \equiv 1 \pmod 6$, and $d = (p-5)/6$ if $p \equiv 5 \pmod 6$. This establishes the theorem. $\square$

In what follows, we concentrate on the case where $m = 1$, that is, on the number $f_\lambda = f_\lambda(1)$ of free subgroups of index 6λ in the modular group $\mathrm{PSL}_2(\mathbb{Z})$. Note that this means that we consider the case of Theorems 1 and 11 where $A = E = 4$, $B = 6$, $C = 1$, and $D = 0$. Our goal is to make Theorem 11 in this special case more explicit for the first few prime numbers, and to determine precisely the (minimal) period length of the sequence $(f_\lambda)_{\lambda\ge1}$ when it is reduced modulo these prime numbers.

Theorem 12. *Let α be a positive integer. Then the generating function $F(z) = 1 + \sum_{\lambda\ge1} f_\lambda z^\lambda$, when coefficients are reduced modulo 7^α, equals $P_\alpha(z)/(1+2z)^\alpha$, where $P_\alpha(z)$ is a polynomial in z over the integers. In particular, the sequence $(f_\lambda)_{\lambda\ge1}$ is ultimately periodic, with minimal period equal to $6 \cdot 7^{\alpha-1}$.*

Proof. In view of Theorem 11, and since $Q_1(z) = 1+2z$ modulo 7 for $A = E = 4$, $B = 6$, $C = 1$, the only assertion which still requires proof is the one about the period length. A careful examination of the previous arguments (see in particular (5.14)) reveals that we have actually shown the stronger statement that the solution $F(z)$ to (4.1) with $m = 1$, when coefficients are reduced modulo 7^α, can be written in the form

$$F(z) = \mathrm{Pol}_\alpha(z) + \sum_{k=1}^{\alpha} f_{-k} 7^{k-1}(1+2z)^{-k} \quad \text{modulo } 7^\alpha,$$

where $\mathrm{Pol}_\alpha(z)$ is a polynomial in z with integer coefficients, and the f_{-k}'s are integers. Now, we have

$$7^{k-1}(1+2z)^{-k} = \sum_{\ell\ge0} (-2)^\ell 7^{k-1} \binom{k+\ell-1}{k-1} z^\ell.$$

The term $(-2)^\ell$, $\ell = 0, 1, \dots$, is periodic modulo 7^α with (minimal) period length $\varphi(7^\alpha) = 6 \cdot 7^{\alpha-1}$, where φ denotes Euler's totient function. Indeed, this holds for $\alpha = 1, 2$ by inspection, and thus for every $\alpha \ge 1$ by a theorem of Gauß concerning existence of primitive roots (cf. e.g. [3, Ch. 2, Sec. 5] or [23, pp. 285–287]). On the other hand, the period length of

$$7^{k-1}\binom{k+\ell-1}{k-1} = 7^{k-1-v_7((k-1)!)}\frac{(k+\ell-1)\cdots(\ell+2)(\ell+1)}{(k-1)!7^{-v_7((k-1)!)}}, \quad \ell = 0, 1, \dots,$$

when considered modulo 7^α, divides $7^{\alpha-1}$ for $k \ge 2$, since

$$k - 1 - v_7((k-1)!) \ge 1$$

for $k \ge 2$. In total,

$$(-2)^\ell 7^{k-1}\binom{k+\ell-1}{k-1}, \quad \ell = 0, 1, \dots,$$

when considered modulo 7^α, is periodic with period length (exactly) $6 \cdot 7^{\alpha-1}$, which implies the corresponding assertion of the theorem. □

We have implemented the algorithm which is implicit in the proof of Theorem 11 (see the Note at the end of the Introduction). As an illustration, the next theorem contains the result for the modulus $7^5 = 16807$.

Theorem 13. *We have*

$$\begin{aligned}
1 &+ \sum_{\lambda\ge1} f_\lambda\, z^\lambda \\
&= 4802z^{25} + 9604z^{23} + 14406z^{22} + 2401z^{21} + 2401z^{20} + 4802z^{19} + 9947z^{18} + 9604z^{17} \\
&\quad + 10290z^{16} + 9947z^{15} + 10976z^{14} + 16464z^{13} + 12691z^{12} + 2940z^{11} + 8918z^{10} \\
&\quad + 15484z^{9} + 8722z^{8} + 4214z^{7} + 10829z^{6} + 6174z^{5} + 406z^{4} + 14896z^{3} + 11102z^{2} \\
&\quad + 14168z + 7 + \frac{16451}{1+2z} + \frac{9562}{(1+2z)^2} + \frac{2450}{(1+2z)^3} + \frac{2744}{(1+2z)^4} + \frac{2401}{(1+2z)^5} \\
&\qquad \text{modulo } 7^5. \quad (5.15)
\end{aligned}$$

The case of powers of 11 can be handled in an analogous way. We content ourselves with stating the corresponding result, leaving the proof to the interested reader.

Theorem 14. *Let α be a positive integer. Then the generating function $F(z) = 1 + \sum_{\lambda\ge1} f_\lambda\, z^\lambda$, when coefficients are reduced modulo 11^α, equals $P_\alpha(z)/(1-z)^\alpha$, where $P_\alpha(z)$ is a polynomial in z over the integers. Moreover, the sequence $(f_\lambda)_{\lambda\ge1}$ is ultimately periodic, with minimal period length equal to $11^{\alpha-1}$.*

Again, we have implemented the algorithm which leads to the above theorem (see the Note at the end of the Introduction). As an illustration, the next theorem contains the result for the modulus $11^5 = 161051$.

Theorem 15. *We have*

$$\begin{aligned}
1 &+ \sum_{\lambda\ge1} f_\lambda\, z^\lambda \\
&= 87846z^{41} + 87846z^{39} + 131769z^{38} + 87846z^{37} + 146410z^{36} + 29282z^{35} + 87846z^{34}
\end{aligned}$$

$$+ 87846z^{33} + 131769z^{32} + 123783z^{30} + 146410z^{29} + 65219z^{28} + 151734z^{27} + 153065z^{26} + 105149z^{25} + 154396z^{24} + 145079z^{23} + 153065z^{22} + 22627z^{21} + 103818z^{20} + 4719z^{19} + 78529z^{18} + 156453z^{17} + 153186z^{16} + 64614z^{15} + 123178z^{14} + 20933z^{13} + 154033z^{12} + 84579z^{11} + 93533z^{10} + 151492z^{9} + 28325z^{8} + 136730z^{7} + 23727z^{6} + 43164z^{5} + 75636z^{4} + 149358z^{3} + 126445z^{2} + 97383z + 7 + \frac{80547}{1-z} + \frac{6809}{(1-z)^2} + \frac{17787}{(1-z)^3} + \frac{41261}{(1-z)^4} + \frac{14641}{(1-z)^5} \quad \text{modulo } 11^5. \tag{5.16}$$

The next prime, 13, is congruent to 1 modulo 6, and Theorem 11 says that we may present the solution modulo 13^e as a rational function with denominator being the e-th power of a quadratic factor. It turns out that this quadratic factor is $(1-2z)(1+5z)$. Experimentally, it seems that the maximal exponent s such that $(1+5z)^{-s}$ appears in the (cleared) denominator is actually $s = (e+1)/2$ (instead of e; see for example Theorem 17), but our methods are not able to demonstrate this. What we are able to prove is summarised in the theorem below.

Theorem 16. *Let α be a positive integer. Then the generating function $F(z) = 1 + \sum_{\lambda\ge1} f_\lambda\, z^\lambda$, when coefficients are reduced modulo 13^α, equals $P_\alpha(z)/\big((1-2z)(1+5z)\big)^\alpha$, where $P_\alpha(z)$ is a polynomial in z over the integers. Moreover, the sequence $(f_\lambda)_{\lambda\ge1}$ is ultimately periodic, with minimal period length equal to $12 \cdot 13^{\alpha-1}$.*

The algorithm which led to the above theorem generates the following result for the modulus $13^5 = 371293$.

Theorem 17. *We have*

$$1 + \sum_{\lambda\ge1} f_\lambda\, z^\lambda = 314171z^{42} + 285610z^{40} + 142805z^{38} + 114244z^{37} + 285610z^{36} + 57122z^{35} + 118638z^{34} + 285610z^{33} + 325156z^{32} + 142805z^{30} + 90077z^{29} + 338338z^{28} + 349323z^{27} + 188942z^{26} + 103259z^{25} + 26364z^{24} + 35152z^{23} + 188942z^{22} + 4732z^{21} + 76895z^{20} + 310622z^{19} + 28561z^{18} + 340535z^{17} + 358787z^{16} + 353379z^{15} + 135031z^{14} + 115596z^{13} + 20280z^{12} + 328874z^{11} + 55939z^{10} + 116441z^{9} + 56745z^{8} + 179309z^{7} + 342212z^{6} + 219700z^{5} + 24336z^{4} + 238953z^{3} + 332462z^{2} + 354965z + 13 + \frac{208033}{1+5z} + \frac{363181}{(1+5z)^2} + \frac{171366}{(1+5z)^3} + \frac{334822}{1-2z} + \frac{176228}{(1-2z)^2} + \frac{154635}{(1-2z)^3} + \frac{134017}{(1-2z)^4} + \frac{314171}{(1-2z)^5} \quad \text{modulo } 13^5. \tag{5.17}$$

For $p = 17$, the denominators of rational solutions to (4.1) with $m = 1$ (viewed modulo a power of p) are powers of $1 + 15z + 7z^2$ (which does not factor modulo 17), and for $p = 19, 23$ they are powers of (irreducible) ternary factors, etc. A generalisation of the argument in the proof of Theorem 12 shows that it is still true that the period of f_λ modulo a prime power p^α is a multiple of $p^{\alpha-1}$, but, which multiple it actually is, is in general difficult to describe. For example, modulo 17 the period of f_λ is $6 \cdot 16$, modulo 17^2 it is $18 \cdot 16 \cdot 17$, while modulo 17^3 it is $102 \cdot 16 \cdot 17^2$.

6. Free subgroup numbers for lifts of $\mathfrak{H}(4)$ modulo prime powers

In this last section, we apply Theorem 1 to the free subgroup numbers of another family of groups: the lifts $\Gamma_m(4)$ of the Hecke group $\mathfrak{H}(4) = C_2 * C_4$ defined by

$$\Gamma_m(4) = C_{2m} \underset{C_m}{*} C_{4m} = \left\langle x, y \,\middle|\, x^{2m} = y^{4m} = 1,\, x^2 = y^4 \right\rangle,$$

where m is a positive integer. Given $\lambda \geq 1$, let $f_\lambda^{(4)}(m)$ denote the number of free subgroups of index $4m\lambda$ in $\Gamma_m(4)$, and let $F_m^{(4)}(z) = 1 + \sum_{\lambda \geq 1} f_\lambda^{(4)}(m) z^\lambda$ be the corresponding generating function. In particular, $f_\lambda^{(4)} := f_\lambda^{(4)}(1)$ is the number of free subgroups of index 4λ in the Hecke group $\mathfrak{H}(4)$.

From the theory developed in [18], it is well-known that $F_m^{(4)}(z)$ satisfies a differential equation. In order to determine the precise form of this differential equation, several invariants of the groups $\Gamma_m(4)$ have to be computed. Following the notation of [18], these are:

$$\begin{aligned} m_{\Gamma_m(4)} &= 4m, \\ \chi(\Gamma_m(4)) &= \frac{1}{2m} + \frac{1}{4m} - \frac{1}{m} = -\frac{1}{4m}, \\ \mu(\Gamma_m(4)) &= 1 - m_{\Gamma_m(4)} \chi(\Gamma_m(4)) = 2, \end{aligned}$$

and the invariants $A_\mu = A_\mu(\Gamma_m(4))$, $0 \leq \mu \leq 2$, for which we obtain

$$A_0 = 3m^2, \quad A_1 = 32m^2, \quad A_2 = 16m^2.$$

The differential equation then becomes[3]

$$(1-(4m-2)z)F_m^{(4)}(z) - 4mz^2(F_m^{(4)})'(z) - z(F_m^{(4)})^2(z) - 1 - (1-4m+3m^2)z = 0. \tag{6.1}$$

Visibly, this is the special case of (2.1) where $A = 4m-2$, $B = 4m$, $C = 1$, and $D = 1-4m+3m^2$. Hence, Theorem 1 applies and allows us to derive results analogous to the ones in Sections 4 and 5 for the lifts of the modular group. Since also the proofs are completely analogous, we content ourselves with just stating these results.

Theorem 18. *Let m be a positive integer, p a prime number with $p \geq 3$, and let α be a positive integer. Then the generating function $F_m^{(4)}(z) = 1 + \sum_{\lambda \geq 1} f_\lambda^{(4)}(m) z^\lambda$, when coefficients are reduced modulo p^α, can be represented as a rational function. Equivalently, the sequence $(f_\lambda^{(4)}(m))_{\lambda \geq 1}$ is ultimately periodic modulo p^α.*

Lemma 19. *Let p be a prime with $p \equiv 1 \pmod 4$. For $A = 4m-2$, $B = 4m$, $C = 1$, $D = 1-4m+3m^2$ (and, hence, $E = 2m$), and $n \equiv \frac{p-1}{4}, \frac{3(p-1)}{4} \pmod p$, we have*

$$Q_n(z) = Q_{(p-1)/4}(z) \quad \text{modulo } p,$$

with $Q_n(z)$ as given in the assertion of Theorem 1. Furthermore, if $p \nmid m$, then the polynomial $Q_{(p-1)/4}(z)$ has degree $(p-1)/4$ in z when coefficients are reduced modulo p, whereas $Q_{(p-1)/4}(z) = 1$ modulo p if $p \mid m$.

[3]Cf. Formula (18) in [18, Sec. 2.3] with $F_m^{(4)}(z) = 1 + z\beta_{\Gamma_m(4)}(z)$ for the result in a more general context.

Lemma 20. *Let p be a prime with $p \equiv 3 \pmod 4$. For $A = 4m-2$, $B = 4m$, $C = 1$, $D = 1 - 4m + 3m^2$ (and, hence, $E = 2m$), and $n \equiv \frac{p-3}{4}, \frac{3p-1}{4} \pmod p$, we have*

$$Q_n(z) = Q_{(p-3)/4}(z) \quad \text{modulo } p,$$

with $Q_n(z)$ as given in Theorem 1. Furthermore, if $p \nmid m$, then the polynomial $Q_{(p-3)/4}(z)$ has degree $(p-3)/4$ in z when coefficients are reduced modulo p, whereas $Q_{(p-3)/4}(z) = 1$ modulo p if $p \mid m$.

Theorem 21. *Let α be a positive integer. If p is a prime with $p \equiv 1 \pmod 4$, then the generating function $F_m^{(4)}(z) = 1 + \sum_{\lambda \ge 1} f_\lambda^{(4)}(m)\, z^\lambda$, when coefficients are reduced modulo p^α, equals $\overline{P}_\alpha(z)/Q^\alpha_{(p-1)/4}(z)$, where $\overline{P}_\alpha(z)$ is a polynomial in z over the integers, and $Q_{(p-1)/4}(z)$ is the polynomial of degree $(p-1)/4$ given by the formula in Theorem 1 with $A = 4m-2$, $B = 4m$, $C = 1$, $D = 1 - 4m + 3m^2$ and $E = 2m$.*

On the other hand, if p is a prime with $p \equiv 3 \pmod 4$, then the generating function $F_m^{(4)}(z) = 1 + \sum_{\lambda \ge 1} f_\lambda^{(4)}(m)\, z^\lambda$, when coefficients are reduced modulo p^α, equals $\widehat{P}_\alpha(z)/Q^\alpha_{(p-3)/4}(z)$, where $\widehat{P}_\alpha(z)$ is a polynomial in z over the integers, and $Q_{(p-3)/4}(z)$ is the polynomial of degree $(p-3)/4$ given by the formula in Theorem 1 with $A = 4m-2$, $B = 4m$, $C = 1$, $D = 1 - 4m + 3m^2$ and $E = 2m$.

Remarks 22. (1) Also in the present context, it would be possible without any additional effort to make Theorem 21 more explicit for concrete primes p; thus obtaining results analogous to the ones in Theorems 12–17. We omit this here for the sake of brevity.

(2) The Riccati differential equation (6.1) is in a form so that the method from [12] for the determination of the behaviour of sequences modulo powers of 2 as well as the method from [15] for the determination of the behaviour of sequences modulo powers of 3 are applicable. Consequently, one could derive results analogous to the ones in [12, Sec. 8] and [15, Sec. 16] for the free subgroup numbers of the lifts $\Gamma_m(3)$ of $\mathrm{PSL}_2(\mathbb{Z})$.

(3) One may speculate that the obvious generalisation of Theorems 8 and 18 may hold for the lifts $\Gamma_m(q)$ of an arbitrary Hecke group $\mathfrak{H}(q)$, given by

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

Computer experiments seem to support this speculation.

Appendix: How were the expressions for $p_{n,k}$ and $q_{n,k}$ found?

When papers get written, the path(s) towards the results presented often get lost, are covered up, or — in some cases — even hidden intentionally. As we believe that, in the present case, this path is actually quite interesting and instructive, we shall describe in this appendix how we were led to conjecture the formulae in (2.3) and (2.4), without which we would not even have been able to prove the mere existence of solutions to (2.2), and without which we would therefore never have reached the result described in Theorem 8 concerning the number of free subgroups in lifts of the inhomogeneous modular group, which was our primary goal and motivation.

Recall that the generating function $F(z) = 1 + \sum_{\lambda \ge 1} f_\lambda\, z^\lambda$, where f_λ denotes again the number of free subgroups of $\mathrm{PSL}_2(\mathbb{Z})$ of index 6λ, satisfies the Riccati differential equation (4.1) with $m = 1$, that is,

$$(1 - 4z)F(z) - 6z^2 F'(z) - zF^2(z) - 1 = 0, \tag{A.1}$$

This equation allows us to compute the numbers f_λ recursively. We started out by looking at tables of these numbers, when they are reduced modulo powers of 5, 7, 11, 13, etc. The case of 5 is a trivial (and exceptional) one, since it is not hard to see that f_λ vanishes modulo any power of 5 once λ is large enough. The next case, powers of 7, is more interesting. Computer experiments quickly led to the conjecture that the free subgroup numbers f_λ modulo a given power of 7 are ultimately periodic, and it was even possible to predict the period length. Theorem 12 presents the precise corresponding statement. Continuing with powers of 11, a similar picture emerged. The precise statement is presented in Theorem 14. With some effort, we could see that the free subgroup numbers f_λ are also periodic when reduced modulo 13 or 17, however with considerably larger period lengths. What happens modulo higher powers of 13 or 17 was unclear at that point.

We then decided to try to prove, say, the statements modulo powers of 7 and 11. An approach in the style of [12] and [15] came quite close, but did not succeed. At some point, we had the idea of "Padé-approximating" the solution to (A.1) by a rational function with numerator and denominator degrees equal to n, and see how far this rational function fails to satisfy the differential equation (A.1). We were (pleasantly) surprised to see that the error on the right-hand side was a "round"[4] multiple of $z^{2n+1}/Q_n^2(z)$, and, using the guessing programme `Rate`,[5] it was not difficult to come up with the conjecture that (4.2) (with $m = 1$) should hold.

After several failed attempts at proving this conjecture, in a mood of despair, we decided to make everything more general, not expecting anything but horrendous results. We put as many parameters as possible into the differential equation (A.1), so that we were led to consider the differential equation (2.1). We were in for another pleasant surprise: although one cannot go very far with nowadays' computers (we only made it up to $n = 5$), the pattern which is displayed in what is now Theorem 1 became quickly clear, however without any clue about the explicit form of the rational function $R_n(z)$. For example, we obtained

$$R_1(z) = \frac{1 + (-B - C + D)z}{1 + (-A - B - 2C)z}, \tag{A.2}$$

$$R_2(z) = \frac{1 + (-A - 4B - 3C + D)z + (-AD + 2B^2 + 3BC - 3BD + C^2 - 3CD)\,z^2}{1 + (-2A - 4B - 4C)z + (A^2 + 3AB + 3AC + 2B^2 + 6BC + 3C^2 - CD)\,z^2}, \tag{A.3}$$

$$R_3(z) = \frac{P_3(z)}{Q_3(z)}, \tag{A.4}$$

[4]According to Hardy [11, Ch. III], "a number is described in popular language as *round* if it is the product of a considerable number of comparatively small factors," which was picked up by Kuperberg [16, Sec. VII.A] (in fact, being unaware of Hardy's statement) in the form "an integer is *round* if it is a product of relatively small (prime) numbers. A round enumeration in combinatorics almost always has an explicit product formula." See [13, Sec. 2] for a more detailed elaboration of the "notion" of "roundness."

[5]written in *Mathematica* by the first author; available from
`http://www.mat.univie.ac.at/~kratt`

with

$$\begin{aligned} P_3(z) = 1 &+ z(-2A - 9B - 5C + D) \\ &+ z^2 \left(A^2 + 7AB + 4AC - 2AD + 18B^2 + 22BC - 8BD + 6C^2 - 6CD\right) \\ &+ z^3\big(A^2D + 6ABD + 4ACD - 6B^3 - 11B^2C + 11B^2D \\ &\qquad - 6BC^2 + 18BCD - C^3 + 6C^2D - CD^2\big) \end{aligned}$$

and

$$\begin{aligned} Q_3(z) = 1 &+ z(-3A - 9B - 6C) \\ &+ z^2 \left(3A^2 + 15AB + 10AC + 18B^2 + 30BC + 10C^2 - 2CD\right) \\ &+ z^3\big(- A^3 - 6A^2B - 4A^2C - 11AB^2 - 18ABC - 6AC^2 + 2ACD - 6B^3 \\ &\qquad - 22B^2C - 18BC^2 + 6BCD - 4C^3 + 4C^2D\big). \end{aligned}$$

On the basis of these computer data (including the ones for $R_4(z)$ and $R_5(z)$), it is not difficult to come up with guesses for the first few coefficients $p_{n,k}$ and $q_{n,k}$:

$$p_{n,1} = -(n-1)A - n^2B - (2n-1)C + D, \tag{A.5}$$

$$q_{n,1} = -nA - n^2B - 2nC, \tag{A.6}$$

$$\begin{aligned} p_{n,2} = &\tfrac{1}{2}(n-2)(n-1)A^2 + \tfrac{1}{2}(n-2)(n-1)(2n+1)AB + 2(n-2)(n-1)AC \\ &- (n-1)AD + \tfrac{1}{2}(n-1)^2n^2B^2 + (n-1)\left(2n^2 - 2n - 1\right) BC \\ &- (n-1)(n+1)BD + (n-1)(2n-3)C^2 - 3(n-1)CD, \end{aligned} \tag{A.7}$$

$$\begin{aligned} q_{n,2} = &\tfrac{1}{2}(n-1)nA^2 + \tfrac{1}{2}(n-1)n(2n-1)AB + (n-1)(2n-1)AC + \tfrac{1}{2}(n-1)^2n^2B^2 \\ &+ (n-1)n(2n-1)BC + (n-1)(2n-1)C^2 - (n-1)CD, \end{aligned} \tag{A.8}$$

$$\begin{aligned} p_{n,3} = &-\tfrac{1}{6}(n-3)(n-2)(n-1)A^3 - \tfrac{1}{2}(n-3)(n-2)\left(n^2 - n - 1\right) A^2B \\ &- \tfrac{1}{2}(n-3)(n-2)(2n-3)A^2C + \tfrac{1}{2}(n-2)(n-1)A^2D \\ &- \tfrac{1}{6}(n-3)(n-2)\left(3n^3 - 3n^2 - n - 2\right) AB^2 \\ &- \tfrac{1}{2}(n-3)(n-2)(2n-3)(2n+1)ABC + \tfrac{1}{2}(n-2)(n+1)(2n-3)ABD \\ &- (n-3)(n-2)(2n-3)AC^2 + (n-2)(3n-5)ACD \\ &- \tfrac{1}{6}(n-2)^2(n-1)^2n^2B^3 - \tfrac{1}{6}(n-2)(2n-3)\left(3n^3 - 6n^2 - n - 2\right) B^2C \\ &+ \tfrac{1}{2}(n-2)\left(n^3 - n - 2\right) B^2D - (n-2)(2n-3)\left(n^2 - 2n - 1\right) BC^2 \\ &+ (n-2)\left(3n^2 - 2n - 3\right) BCD - \tfrac{1}{3}(n-2)(2n-5)(2n-3)C^3 \\ &+ 2(n-2)(2n-3)DC^2 - (n-2)CD^2, \end{aligned} \tag{A.9}$$

$$\begin{aligned} q_{n,3} = &-\tfrac{1}{6}(n-2)(n-1)nA^3 - \tfrac{1}{2}(n-2)(n-1)^2nA^2B - (n-2)(n-1)^2A^2C \\ &- \tfrac{1}{6}(n-2)(n-1)n\left(3n^2 - 6n + 2\right) AB^2 - (n-2)(n-1)n(2n-3)ABC \\ &- (n-2)(n-1)(2n-3)AC^2 + (n-2)(n-1)ACD \\ &- \tfrac{1}{6}(n-2)^2(n-1)^2n^2B^3 - \tfrac{1}{3}(n-2)(n-1)n\left(3n^2 - 6n + 2\right) B^2C \\ &- (n-2)(n-1)n(2n-3)BC^2 + (n-2)(n-1)nBCD \\ &- \tfrac{2}{3}(n-2)(n-1)(2n-3)C^3 + 2(n-2)(n-1)C^2D. \end{aligned} \tag{A.10}$$

So, it seemed "clear" that the $p_{n,k}$'s and $q_{n,k}$'s were homogeneous polynomials in A, B, C, D of degree k. However, having stared at this for some while, it seemed hopeless to us to continue along these lines.

We made the "intermediate" observation that, should we be able to demonstrate something at all in this context, it would have to come from the "hypergeometric world," and consequently the quadratic factors in the right-hand side product of (2.2) must factor into linear factors. This happens only if the discriminant of the factor, viewed as a quadratic form in ℓ, has a square root, and the latter requires the parametrisation $E^2 = A^2 - 4CD$. If one uses this parametrisation, then the right-hand side product in (2.2) becomes

$$-(A+C+D)\prod_{\ell=1}^{n}(\ell AB + AC + CD + \ell^2B^2 + 2\ell BC + C^2) = -\frac{1}{C}\Pi_+\Pi_-,$$

where, again, we make use of the short-hand notation in (3.2).

At a certain point, we decided to "look at the other end," that is, to try to find formulae for the coefficients $p_{n,k}$ and $q_{n,k}$ for $k = n, n-1, \dots$ Comparing coefficients of z^{2n+1} on both sides of (3.1), one obtains the equation

$$-Ap_{n,n}q_{n,n} - Cp_{n,n}^2 - Dq_{n,n}^2 = -\frac{1}{C}\Pi_+\Pi_-.$$

Moreover, upon using the parametrisation $E^2 = A^2 - 4CD$, the left-hand side factors, leading to

$$\left(Cp_{n,n} + \tfrac{1}{2}(A-E)q_{n,n}\right)\left(Cp_{n,n} + \tfrac{1}{2}(A+E)q_{n,n}\right) = \Pi_+\Pi_-.$$

If there is any "justice" in the world, then one of the factors on the left-hand side would have to agree with one of the factors on the right-hand side, and the same should hold for the other two factors. Indeed, the computer told us that, apparently,

$$\begin{aligned} Cp_{n,n} + \tfrac{1}{2}(A-E)q_{n,n} &= \Pi_-,\\ Cp_{n,n} + \tfrac{1}{2}(A+E)q_{n,n} &= \Pi_+. \end{aligned}$$

Solving this system of linear equations for $p_{n,n}$ and $q_{n,n}$, one arrives at

$$p_{n,n} = \frac{(-1)^{n+1}}{2CE}\big((A-E)\Pi_+ - (A+E)\Pi_-\big)$$

(that is, Equation (3.3)), and

$$q_{n,n} = \frac{(-1)^n}{E}(\Pi_+ - \Pi_-)$$

(that is, Equation (3.4)).

Subsequently, we proceeded to compare coefficients of z^{2n} on both sides of (3.1). This leads to a linear equation for $p_{n,n-1}$ and $q_{n,n-1}$, with coefficients containing Π_+ and Π_-. Containing two unknowns, it is certainly undetermined. Nevertheless, one is able to come up with a guess: one considers the equation first modulo $\Pi_+ - \Pi_-$, and then modulo $\Pi_+ + \Pi_-$. As it turns out, this leads to dramatic simplification, and one obtains two *linear* congruences for $p_{n,n-1}$ and $q_{n,n-1}$ (the moduli being $\Pi_+ - \Pi_-$ and $\Pi_+ + \Pi_-$, respectively), with coefficients being rational functions in A, B, C, E. One can then again use computer experiments to come up with a guess for the multiplicative factors which make these congruences into equations. Once this is done, one has two linear equations, which one solves for $p_{n,n-1}$ and $q_{n,n-1}$. The result was (2.3) and (2.4) with $k=1$ (albeit not yet written in this form). We did the same for $p_{n,n-2}$ and $q_{n,n-2}$, and for $p_{n,n-3}$ and $q_{n,n-3}$. (The latter required to also compute $R_6(z)$ and $R_7(z)$, which now, by putting the knowledge of the coefficients $p_{n,k}$ and $q_{n,k}$ for $k=n,n-1,n-2$ into the computer programme, became feasible.)

At this stage, we realised that the coefficients of Π_+ and Π_- became "elegant," if one expanded them — viewed as polynomials in n — in the basis

$$1,\ (n-k+1),\ (n-k+1)(n-k+2),\ \dots,\ (n-k+1)(n-k+2)\cdots(n-1)n.$$

We also had at this stage abundant "information" on the arising denominators and signs. More precisely, our experimental data told us that one could apparently write

$$\begin{aligned}p_{n,n-k}=&\frac{(-1)^{n+1}B^{n-k}}{2C\,(\frac{E}{B}-k)_{2k+1}}\\ &\times\Bigg(\left(\tfrac{A+2C+E}{2B}\right)_{n+1}\sum_{j=0}^{k}(n-k+1)_{k-j}\left(-\tfrac{E}{B}+j+1\right)_{k-j}\left(\tfrac{A+2C-E}{2B}\right)_j\\ &\qquad\qquad\cdot\left(p^{(1)}_{n,k,j}A+p^{(2)}_{n,k,j}B-p^{(3)}_{n,k,j}E\right)\\ &\quad-\left(\tfrac{A+2C-E}{2B}\right)_{n+1}\sum_{j=0}^{k}(n-k+1)_{k-j}\left(\tfrac{E}{B}+j+1\right)_{k-j}\left(\tfrac{A+2C+E}{2B}\right)_j\\ &\qquad\qquad\cdot\left(p^{(1)}_{n,k,j}A+p^{(2)}_{n,k,j}B+p^{(3)}_{n,k,j}E\right)\Bigg)\end{aligned}$$

and

$$\begin{aligned}q_{n,n-k}=&\frac{(-1)^{n}B^{n-k}}{(\frac{E}{B}-k)_{2k+1}}\\ &\times\Bigg(\left(\tfrac{A+2C+E}{2B}\right)_{n+1}\sum_{j=0}^{k}q_{n,k,j}(n-k+1)_{k-j}\left(-\tfrac{E}{B}+j+1\right)_{k-j}\left(\tfrac{A+2C-E}{2B}\right)_j\\ &\quad-\left(\tfrac{A+2C-E}{2B}\right)_{n+1}\sum_{j=0}^{k}q_{n,k,j}(n-k+1)_{k-j}\left(\tfrac{E}{B}+j+1\right)_{k-j}\left(\tfrac{A+2C+E}{2B}\right)_j\Bigg),\end{aligned}\tag{A.11}$$

with "nice" numerical coefficients $p^{(1)}_{n,k,j},p^{(2)}_{n,k,j},p^{(3)}_{n,k,j},q_{n,k,j}$. The available data at this point (namely, the rational functions $R_n(z)$ for $n=1,2,\dots,7$) were largely insufficient to make any guesses about these coefficients. However, assuming the above forms of $p_{n,k}$ and $q_{n,k}$, together with the earlier observed polynomiality of $p_{n,k}$ and $q_{n,k}$ in A,B,C,D, and, hence, also in A,B,C,E (except for possible powers of C in denominators), sufficient data could now be easily produced! Let us first concentrate on $q_{n,n-k}$ (as we did). If $q_{n,n-k}$ is to be a polynomial, then $(\frac{E}{B}-k)_{2k+1}$ must divide the expression between parentheses on the right-hand side of (A.11), that is, this expression must vanish for $E=Bs$, $s=-k,-k+1,\dots,k$. Let us do the substitution $E=Bs$ in this expression, and let us suppose that $s>0$. Then we have

$$\left(\tfrac{A+2C+E}{2B}\right)_{n+1}=\left(\tfrac{A+2C+Bs}{2B}\right)_{n+1}=\left(\tfrac{A+2C+Bs}{2B}\right)_{n+1-s}\left(\tfrac{A+2C-Bs}{2B}+n+1\right)_s.$$

Comparing with

$$\left(\tfrac{A+2C-E}{2B}\right)_{n+1} = \left(\tfrac{A+2C-Bs}{2B}\right)_{n+1},$$

we infer that $\left(\tfrac{A+2C-Bs}{2B}+n+1\right)_s$ must divide the second sum over j *as a polynomial in* n. This provides many non-trivial vanishing conditions for this sum over j, viewed as polynomial in n (they actually "overdetermine" it), and this suffices to compute the coefficients $q_{n,k,j}$ for a large range of k's and corresponding j's. Using the guessing programme `Rate` (see Footnote 5) once again, it is then straightforward to guess the formula in (2.4). For the coefficients $p^{(1)}_{n,k,j}, p^{(2)}_{n,k,j}, p^{(3)}_{n,k,j}$ one does not have to do the same work again: it suffices to look at the quotients

$$\frac{p^{(1)}_{n,k,j}}{q_{n,k,j}}, \frac{p^{(2)}_{n,k,j}}{q_{n,k,j}}, \frac{p^{(3)}_{n,k,j}}{q_{n,k,j}},$$

which quickly leads one to the formula in (2.3).

References

[1] W. N. Bailey, *Generalized Hypergeometric Series*, Cambridge University Press, Cambridge, 1935.

[2] G. A. Baker, Jr. and P. R. Graves-Morris, *Padé Approximants*, Cambridge University Press, Cambridge, 1996.

[3] P. Bundschuh, *Einführung in die Zahlentheorie*, Springer-Verlag, Berlin, 1992.

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

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

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

[7] R. W. Gosper, Decision procedure for indefinite hypergeometric summation, *Proc. Natl. Acad. Sci. USA* **75** (1978), 40–42.

[8] R. L. Graham, D. E. Knuth and O. Patashnik, *Concrete Mathematics*, Addison-Wesley, Reading, Massachusetts, 1989.

[9] P. Hall, A contribution to the theory of groups of prime-power order, *Proc. Lond. Math. Soc.* (2) **36** (1934), 29–95.

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

[11] G. H. Hardy, *Ramanujan*, twelve lectures on subjects suggested by his life and work, Chelsea Publ. Comp., New York, 1940.

[12] M. Kauers, C. Krattenthaler and T. W. Müller, A method for determining the mod-2^k behaviour of recursive sequences, with applications to subgroup counting, *Electron. J. Combin.* **18**(2) (2012), Article P37, 83 pp.

[13] C. Krattenthaler, Advanced determinant calculus: a complement, *Linear Algebra Appl.* **411** (2005), 68–166.

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

[15] C. Krattenthaler and T. W. Müller, A method for determining the mod-3^k behaviour of recursive sequences, preprint, 2012.

[16] G. Kuperberg, An exploration of the permanent-determinant method, *Electron. J. Combin.* **5** (1998), Article #R46, 34 pp.

[17] A. M. Legendre, *Essai sur la théorie des nombres*, 2$^{\text{e}}$ ed., Courcier, Paris, 1808.

[18] 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, pp. 327–374.

[19] T. W. Müller, Modular subgroup arithmetic and a theorem of Philip Hall, *Bull. London Math. Soc.* **34** (2002), 587–598.
[20] T. W. Müller, Modular subgroup arithmetic in free products, *Forum Math.* **15** (2003), 759–810.
[21] T. W. Müller and J.-C. Schlage-Puchta, Modular arithmetic of free subgroups, *Forum Math.* **17** (2005), 375–405.
[22] 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.
[23] O. Ore, *Number Theory And Its History*, Dover Publ. Inc., New York, 1988.
[24] M. Petkovšek, H. Wilf and D. Zeilberger, $A{=}B$, A. K. Peters, Wellesley, 1996.
[25] L. J. Slater, *Generalized Hypergeometric Functions*, Cambridge University Press, Cambridge, 1966.
[26] L. Sylow, Théorèmes sur les groupes de substitutions, *Math. Ann.* **5** (1872), 584–594.

†*Fakultät für Mathematik, Universität Wien, Nordbergstrasze 15, A-1090 Vienna, Austria. WWW: `http://www.mat.univie.ac.at/~kratt`.

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